2020-12

SIGNALING FOR COERCION IN CYBERSPACE

Longabaugh, Eric E.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SIGNALING FOR COERCION IN CYBERSPACE

by

Eric E. Longabaugh

December 2020

Thesis Advisor: Wade L. Huntley
Second Reader: Michael Senft

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
SIGNALING FOR COERCION IN CYBERSPACE

5. FUNDING NUMBERS

6. AUTHOR(S) Eric E. Longabaugh

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

In order for signaling to work on an adversary with a coercive purpose, one must convey to the adversary a strong capability and sufficient credibility. The reason deterrence worked in the Gulf War was that U.S. policymakers had a well-established and highly feared capability in hand, and establishing credibility was the primary concern in that scenario. However, cyber-based capabilities have not reached a potency to where they could coerce an adversary in and of themselves. The failure of the coalition to compel Saddam Hussein to withdraw from Kuwait underscores the limits of compellence even when based on overwhelming conventional force; cyber capabilities are still not comparable to conventional forces in hurting power, which undermines their viability for coercion. Credibility is not an issue; the history of cyber conflict demonstrates that the only way nations establish capability is by the actual employment of capabilities against adversary targets, which solves the problem of credibility. Yet the most powerful cyber effects on critical infrastructure, such as those demonstrated in the Stuxnet attack, cannot permanently disarm an adversary and run the risk of escalation into a kinetic war. Research for this thesis indicates that signaling in cyberspace to an adversary for the intent of coercion is possible but unlikely to succeed while cyberweapons lack the capability to inflict sufficient harm on the adversary.

14. SUBJECT TERMS
coercion, deterrence, cyberspace, signaling, persistent engagement, compellence

15. NUMBER OF PAGES
73

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SIGNALING FOR COERCION IN CYBERSPACE

Eric E. Longabaugh
Lieutenant, United States Navy
BS, U.S. Naval Academy, 2015

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
December 2020

Approved by: Wade L. Huntley
Advisor

Michael Senft
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In order for signaling to work on an adversary with a coercive purpose, one must convey to the adversary a strong capability and sufficient credibility. The reason deterrence worked in the Gulf War was that U.S. policymakers had a well-established and highly feared capability in hand, and establishing credibility was the primary concern in that scenario. However, cyber-based capabilities have not reached a potency to where they could coerce an adversary in and of themselves. The failure of the coalition to compel Saddam Hussein to withdraw from Kuwait underscores the limits of compellence even when based on overwhelming conventional force; cyber capabilities are still not comparable to conventional forces in hurting power, which undermines their viability for coercion. Credibility is not an issue; the history of cyber conflict demonstrates that the only way nations establish capability is by the actual employment of capabilities against adversary targets, which solves the problem of credibility. Yet the most powerful cyber effects on critical infrastructure, such as those demonstrated in the Stuxnet attack, cannot permanently disarm an adversary and run the risk of escalation into a kinetic war. Research for this thesis indicates that signaling in cyberspace to an adversary for the intent of coercion is possible but unlikely to succeed while cyberweapons lack the capability to inflict sufficient harm on the adversary.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APT	advanced persistent threat
DDoS	distributed denial of service
DHS	Department of Homeland Security
DNC	Democratic National Convention
GRU	Main Intelligence Directorate
IADS	integrated air defense system
IP	Internet Protocol
IRA	Internet Research Agency
IRGC	Iranian Revolutionary Guard Corps
NATO	North Atlantic Treaty Organization
ODNI	Office of the Director of National Intelligence
OPM	Office of Personnel Management
TTP	tactics, techniques, and procedures
USCYBERCOM	U.S. Cyber Command
WMD	weapon of mass destruction

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The purpose of this thesis is to determine if it is possible to successfully signal cyber capabilities to an adversary for the establishment of deterrence in cyberspace. To do so, the thesis draws upon lessons from historical cases of cyber conflict as well as conventional and nuclear deterrence in the 1991 Gulf War. Signaling to an adversary that (1) you can attribute any attack to them, (2) you can hold their targets at risk, and (3) you can do so repeatedly, provide a foundation for deterrence [1]. This study demonstrates that it is possible to signal an adversary for all three in cyberspace. However, because the core message of coercion relies upon a threat of punishment, and because cyber capabilities lack the ability to sufficiently punish or hurt adversaries, the thesis explains why brandishing capabilities in cyberspace will not result in stable deterrence, only escalation. These findings lead to the conclusion that brandishing cyber capabilities to create deterrence is not feasible. The adoption of a strategy of persistent engagement, as opposed to relying on deterrence, is likely the best option available to policymakers at this point in the development of cyberspace as a warfighting domain. Within a strategy of persistent engagement, the role of brandishing cyber capabilities likely has utility to support conventional deterrence by conveying credibility and resolve in a non-lethal and non-escalatory manner; brandishing in cyberspace may also have a role in covert signaling intent and resolve to adversaries and allies. This research recommends that U.S. policy continue to be re-oriented toward a strategy of persistent engagement, and that further research be done into the long-term potential of persistent engagement to shape the norms of behavior in cyberspace.

References

[1] M. C. Libicki, “Brandishing Cyber Capabilities,” RAND, Arlington, VA, USA, 2013.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my adviser, Dr. Wade Huntley, and my second reader, LTC Michael Senft, for their assistance in the production of this thesis, as their direction and feedback were absolutely necessary to its completion. I would like to thank my classmates here at NPS, without whose support this would have been far more difficult. Finally, I would like to thank my family and friends for their prayers and support throughout the course of this work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THE CYBERSPACE SIGNALING PROBLEM

A. INTRODUCTION AND PROBLEM DISCUSSION: THE IMPORTANCE OF SIGNALING

The question of deterrence in cyberspace is a relatively recent issue to the minds of strategic thinkers and policymakers. For the first time in the history of warfare, cyberspace plays a prominent role in the political and military operations of nation-states attempting to achieve their geopolitical goals. In light of this trend, U.S. policymakers have advocated a strategy of deterrence in order to dissuade adversaries from attacking U.S. interests in cyberspace, in some ways similar to the nuclear deterrence strategy implemented in the Cold War. Lieutenant General Stephen Fogarty, the commander of U.S. Army Cyber Command, wrote in an article written for the summer 2020 *Cyber Defense Review*: "Deterrence requires communication. Adversaries obviously will not be deterred by capabilities we have that they do not know about. The Army must establish command and control mechanisms, ensure interoperability, and protect forward presence forces (including cyber and information protection) that achieve deterrence" [2]. Finally, both Senator Angus King and Representative Mike Gallagher, the co-chairmen of the 2020 Cyberspace Solarium Commission, advocate a strategy of layered deterrence, with the goal of signaling to adversaries that the costs of attacking via cyberspace outweigh the benefits they seek to gain by doing so: "This posture [of layered deterrence] signals to adversaries that the U.S. government will respond to cyberattacks, even those below the level of armed conflict that do not cause physical destruction or death, with all the tools at its disposal and consistent with international law" [3].

The previous statements by senior policymakers and thinkers all reference a key pillar needed to establish deterrence: the need to signal or brandish to adversaries that you, the defender, are both willing to and capable of inflicting a high enough cost on them that they will be dissuaded from attacking in the first place. The following research seeks to focus on this key aspect of deterrence in cyberspace. The events that have taken place in Georgia, Estonia, Crimea, eastern Ukraine, and the multiple instances of Russian interference in U.S. domestic politics all demonstrate that efforts of creating stable deterrence against Russian

aggression, if any existed, have failed. Clear and effective signaling of a threatened response using cyber capabilities targeted at a specific actor, should an established threshold of aggressive behavior be crossed, may be what is lacking to create stable deterrence in cyberspace. If effective signaling for deterrence can be achieved, it may help inform U.S. policymakers in creating a viable strategy of deterrence in the cyber domain against great power competitors such as Russia.

B. OVERVIEW OF DETERRENCE THEORY

1. Deterrence and Signaling Fundamentals

A brief overview of deterrence and coercion theory is necessary to frame the issue of signaling and provide perspective. Deterrence is achieved when an actor effectively communicates a credible and potent retaliatory threat to an actor, which then deters the targeted actor from taking any action against the interests of the signaling actor when the retaliatory costs exceed the benefits of the action. The credibility of a threat is a function of capability and intent. In other words, achieving this state of deterrence is only possible if the initiating actor effectively communicates and convinces the target actor both of its capability and willingness to employ said capability. In Chapter II of his study of the cyber conflicts in Estonia and Georgia, Christopher Wrenn describes deterrence as being offensive (or retaliatory) in nature, and has seven general requirements in order to be effective: attribution, threat, communication, credibility, will, and transparency [4]. Wrenn states that one has to be able to correctly attribute an attack to an actor (or has to convince the actor that you can), has to convince the actor that you pose a real threat, is able to communicate a credible threat to a target actor, and can display the political will to retaliate if attacked [4]. Transparency is a key element of communication, as the attacker needs to be able to see what the deterring party is capable of doing, and also the clear threshold of behavior or aggression which must not be crossed in order to not incur the devastating threat promised by the adversary.

The concept of coercion is distinct from that of defense, sometimes called “deterrence by denial.” A strategy of defense consists of relying on capabilities that provide protection against any enemy attack. Any attacker viewing the defensive capabilities of their intended victim could be deterred if the chances of success are too small to justify any attempt – hence

the concept of deterrence by denial. The difference, however, is that a strategy of defense implies that if the defender is convinced of his defensive power to resist any attack, he doesn't need deterrence, though he may want it for other reasons. A defender confident in the capabilities of denial may be indifferent to attack, or may even perceive advantages of allowing the adversary to attack, such as forcing the adversary to reveal tactics or waste resources. However, deterrence is different in that it seeks to forestall any such attack or conflict from ever taking place.

Compellence, closely related to deterrence, uses the threat of force to persuade a victim or adversary to do something they would not otherwise do, and seeks to change the status quo in one's own favor. In the words of Thomas Schelling, deterrence and compellence are both founded in the threat of damage, or of threatening more damage to come: "It is latent violence that can influence someone's choice – violence that can still be withheld or inflicted, or that a victim believes can be withheld or inflicted. The threat of pain tries to structure someone's motives, while brute force tries to overcome his strength" [5]. Thomas Schelling describes deterrence as being relatively simple in that it is mostly indefinite in length of time and easy to communicate as a threat to the adversary; setting a minefield and laying out a tripwire make the threshold past which an adversary should never cross abundantly clear, and is easier to maintain indefinitely. Compellence, on the other hand, requires more communication [5]. Driving a car at someone with the intent of having them get out of the way requires the one driving to somehow communicate to the bystander how long they have to get out of the way, how far they have to move before they are safe, and other more specific conditions for it to work without the car or the person being damaged [5]. For example, there was no doubt about the purpose of American forces in West Germany in the Cold War, or what would cause them to go into action. However, if it ever attacked East Germany, the Warsaw Pact would not from the outset know what would necessarily convince them stop; it would have to be credibly communicated to them for it to be effective [5].

The reason these distinctions are important is the tendency to misapply terminology and frame issues in ways that only create confusion. For example, the 2007 Estonia crisis and 2008 Georgia crisis have both been widely viewed as examples of a failure of deterrence. Those who see these two crises as a failure of U.S. and NATO strategies of cyber deterrence

overlook that there was no deterrence strategy against Russia in the first place [4]. There was no prior signaling or communication on the part of Georgia or Estonia, or by the U.S. on their behalf, to attempt to convince Russia that any attack from cyberspace would result in devastating consequences. The only deterrence at work was in the case of Estonia; being a member of NATO meant that any armed attack against would cause Article 5, the mutual defense provision of the North Atlantic Treaty, to take effect [6]. NATO did not consider the cyberattacks to rise to the level of the use of armed force. Even this implicit deterrence did not apply during the conventional war that Russia waged against Georgia, which was not a member of NATO (This case is discussed in more detail in Chapter II). If no effort was made to deter Russia in the first place, there was no deterrence that could fail. Correct usage of terminology and a careful appreciation of the historical cases are key for any productive discussion on the subject.

The concept of signaling is foundational to the concept of coercion. Signaling or brandishing can be used to convey resolve, used to indicate anger or displeasure over the actions of other nations, or deter or coerce an adversary to alter their calculus and bend them to the will of the signaler. The target of the signal needs to be evident from either the statements made by senior national leaders, or from the context of the actions used in the attempt at signaling. Signaling may only consist of the statements or rhetoric of senior national decisionmakers, but because talking is cheap, signaling seems to be more effective when nations reposition military combat power or resources. Acts such as these are expensive and take time and resources, which convey credibility and resolve to any signaling that may take place. For example, in 1948 the United States signaled serious concern for the situation in Europe to the Soviet Union by sending nuclear-capable bombers to the United Kingdom [7]. The parts necessary for signaling are a signaler (a party that wants to send a message), an intended recipient, an actual signal with an overt or implied message about the actions of the recipient or target, and then feedback to the signaler on whether the message was received [8]. If the signal is not strong enough or not perceived as credible, it may have no effect, encourage the targeted adversary to be more aggressive, or be missed entirely by the intended recipient.

2. Cyber Deterrence

There is a myriad of issues present in the realm of cyber strategy and cyber deterrence which make it more difficult than nuclear deterrence. Martin Libicki, in his foundational work "Cyberdeterrence and Cyberwar," lists attribution, the ability to hold enemy assets at risk, and the need to be able to continuously hold those assets at risk repeatedly -- or at least convincing an adversary that you are capable of doing all three -- as the critical barriers to a viable strategy of deterrence in cyberspace [9]. These three "barriers" to deterrence have negative impacts on the ability to maintain both credibility in the eyes of the adversary and the capabilities to inflict a sufficient amount of damage; both are foundational to signaling for deterrence.

Attribution is a difficult requirement in the context of cyberwar for several reasons. First, one has to be able to effectively distinguish the effects of a cyberattack from a normal IT malfunction [9]. An attack that disrupts the operations of an industrial control system (ICS) could easily be mistaken by the operators as an equipment malfunction or a network failure; such attacks can be designed to appear to be malfunctions or operator errors. The Stuxnet attack, which is discussed in more detail in Chapter II, was an example of this type of obfuscation. The Stuxnet malware was designed to maliciously impact its target while telling the facility operators that operations were normal; because of this any malfunctions were thought to be a result of faulty equipment until the virus was accidentally leaked [10]. Conversely, an actual IT or equipment failure in a system designated as critical infrastructure by the state in which it resides may be mistaken for a cyberattack, and lead to aggressive actions against actors that had nothing to do with the failure. The process of distinguishing between an attack and a malfunction takes time, on top of the time needed to determine who the responsible party is. Timeliness is key for attribution, as any retaliation by the victim against the attacker which occurs well past the date of the initial attack is more likely to be construed as unjustified aggression than retaliation. In order for deterrence to work, the deterring party has to be able to convince any attacker that he (the deterrer) can quickly and accurately attribute the source of a cyberattack [9].

An added concern related to the need for attribution of cyberattacks is the activity of non-state actors as proxies for state actors [7]. Martin Libicki points out that non-state actors may not be officially associated with the government of a state, but may be closely tied with

a political party or a political official within that state, and so conduct external cyberattacks against other nation-states on behalf of that state (like Estonia in 2007) in order to provide a layer of detachment of responsibility. At what point can the actions of those parties be attributed by association to the nation-state to which they belong? If the deterrer cannot establish a tangible link between the non-state actor and the state behind that proxy, this has a further negative impact on the credibility of the deterrer's punishment threat [7].

The second main concern raised by Libicki, the ability to retaliate effectively against any attacker and hold their assets at risk, also raises problems unique to cyberwar [9]. Different countries and actors have varying degrees of vulnerability to cyberattack, a stark contrast from the nuclear age. In the Estonia conflict (evaluated in Chapter II), the cyberattacks coming from Russia were devastating to the operation of that country because of the high dependence that country had on Internet functionality. Conversely, North Korea does not have very many targets of importance that can be touched by cyberattack. A study conducted by a student at the U.S. Naval Postgraduate School revealed that, as of 2015, Internet access in North Korea was limited to a very few high-level government officials: "Use of the Internet in North Korea is strictly controlled by the North Korean government, and users are estimated to be only hundreds of high-ranked officials. Furthermore, because they have an electrical power shortage, operating hours are limited" [11]. This leaves very few options for the U.S. to coerce North Korea using solely cyberattacks.

Additionally, up to this point there have not been any cyberattacks serious enough to have warranted a drastic U.S. response. Cyberattacks and their effects occur for the most part at a purely informational level, and by and large cause little to no physical harm or structural damage. If adversaries know they can weather most attacks in cyberspace, then even if the deterrer has obtained perfect credibility, no adversary will be deterred by retaliation that is restricted only to cyberspace. This opens the question to whether or not cross-domain capabilities (kinetic, economic, diplomatic, etc.) are needed to augment a strategy of cyber deterrence. Wyatt Hoffman concludes as much, and states: "[Cyber warfare] has become a necessary component of warfighting – yet is insufficient by itself. There is an emerging consensus that cyber tools are best used in combination with other instruments" [12]. Yet, despite the increasing inclusion of cyber capabilities in broader military operations, use of

force in response to most independent cyberattacks would be escalatory, increasing the burden of making such a threat credible.

The one counterpoint to this is the growing cyber threat to critical infrastructure, manifested in attacks such as Stuxnet or the BlackEnergy attacks on the Ukrainian power grid. Both of these are examples of malware that had real-world effects and caused significant infrastructural damage with financial and political consequences. Such attacks might be considered grave enough that a use of kinetic force to respond would not be escalatory, in which case kinetic threats to establish deterrence in cyber space may be more credible. The problem of holding adversary targets at risk for this purpose may diminish, as the world as a whole becomes more dependent on information networks and therefore increases the potential surface area of attack via cyberspace. For less grave cyberattacks, however, the escalatory nature of kinetic retaliation may undermine the credibility of kinetic punishment threats for deterrence.

Finally, the question of whether or not one can continuously hold assets at risk makes cyber deterrence uniquely problematic, especially when it comes to demonstrating cyber capabilities with the intent of signaling for deterrence. Most forms of deterrence and warfare are built around capabilities that can be used repeatedly. In cyberwarfare almost all forms of attack depend on a corresponding vulnerability in any given target network. This means that any potential demonstration or use of such a cyber capability to deter an adversary will likely render that capability useless after the first time it is demonstrated, based on the ability of the adversary to patch said vulnerability. It is a relatively easy task to penetrate a network, conduct espionage, and potentially render it useless for a short period of time. However, as Libicki points out in *Cyberspace in Peace and War*, truly damaging attacks such as the Stuxnet malware require a host of dedicated resources, reconnaissance, and personnel to implement successfully [7], [13]. Recall from the Stuxnet case study the many factors and time it took for that effort to be successful. Any one of the vulnerabilities being patched would undermine the malware's ability to achieve its goal, and one may not always have access to the facility with human intelligence assets for reconnaissance and malware insertion. Deterrence requires a continuous ability to hold assets at risk, and if the very act of using a cyber capability puts

its future utility in question, then demonstrating that capability for the purpose of creating deterrence would likely be counterproductive.

C. CYBER DETERRENCE AND SIGNALING

On the specific question of this thesis, concerning the challenge of signaling to establish deterrence in the cyber domain, the two foundational works on which this thesis seeks to build are the monograph "Brandishing Cyberattack Capabilities," written by Martin Libicki, and the article "The Cartwright Conjecture," by Jason Healy. These works focus on the benefits and challenges associated with signaling for deterrence in cyberspace, and seem to the researcher to be the most comprehensive works associated with the topic. Healy's and Libicki's ideas will be the framework from which this thesis develops its further examination of the topic of signaling.

1. Brandishing Cyberattack Capabilities

In "Brandishing Cyberattack Capabilities," Libicki describes the possible benefits and drawbacks of using cyberweapons or capabilities in the context of strategic deterrence [1]. Brandishing capabilities is meant to signal to adversaries that one has the cyber capabilities to exact punishment if certain thresholds of aggressive behavior are crossed. In cyber conflict, there are several difficulties with brandishing effectively. Libicki points out that, while the act of breaking into an adversary's network and leaving a message may seem like a simple task at face-value, the reality is more complicated. He goes on to say that the cyberspace target must be considered by the adversary as sufficiently secure enough to cause great concern if that target was compromised [1]. The nature of high-value targets in cyberspace is that they are very difficult to penetrate, and even more difficult to break. Also of concern is the fact that the success of a cyberattack is dependent upon there being vulnerabilities in the adversary networks and software to properly exploit. Maybe most importantly, a cyberattack that is intended to be seen by the adversary will give the enemy system administrators a very good idea of what vulnerabilities were exploited, and will lead to those crucial vulnerabilities being patched; this is especially true of high-value networks or critical infrastructure. Libicki states that effective brandishing can only take place if the cyberattack capabilities are shown as being able to hold adversary assets at risk repeatedly, so that any actions taken by the adversary to

blunt those capabilities are seen as futile [1]. If resorting to overt displays of cyber capabilities also gives the adversary an idea of how to nullify them, it may not be in the best interest to brandish those capabilities at all [1].

Another issue of concern raised by Libicki is the uncertain ability of cyberweapons to cause lasting or permanent harm [1]. Related to his previous point, if an adversary worries only about a prolonged assault of cyberattacks will diminish its effectiveness over time, it may decide that it can withstand the effects of any initial attack, and patch vulnerabilities as they become known over the course of the exchange [1]. The effectiveness of cyber capabilities in general may vary in relation to how dependent the adversary society or military is on its networks [1]. Libicki points out that that the way in which a capability is brandished will also directly affect its coercive power. For example, an attack that compromises highly-sensitive networks that are visible only to senior adversary decisionmakers and not to the public at large may allow for that decisionmaker to yield to coercion without fear of losing face [1]. Direct intimidation is also a potential option, if the one trying to brandish capabilities can do so in a way that the attack causes far less damage than it potentially could have [1], [5]. All potential methods of brandishing run the risk of provoking a response out of anger or need to demonstrate strength [1]. If a target has a threshold for sensitivity to damage that is greater than its threshold for having to respond to an attack, then any attempt at coercion will fail for either not being painful enough, or provoke a retaliation for being too costly. Finally, Libicki states that brandishing a cyber capability may cause the intended audience to be even less deterred, if they view the use of cyber capabilities as a sign that the attacker is too weak in other domains of warfare [1].

Libicki maintains that there are promising elements to brandishing cyber capabilities [1]. He mentions the fact that the Stuxnet virus has convinced many that the United States is capable of very sophisticated attacks in cyberspace, even though the U.S. has not officially acknowledged a role in its creation or use. However, the impact of brandishing cyber capabilities is highly dependent upon the qualities of the intended target, and the various adversary thresholds for receiving punishment and for retaliation [1]. For this reason, Libicki did not believe that a cyber arms race was likely to characterize the cyber environment, and that a competition to reduce vulnerabilities in systems is more likely than a race to find them.

Libicki's conclusion is that the dangers of unintended consequences in response to signaling with a cyber capability, combined with their lack of power to coerce, make the concept of brandishing a cyberweapon for creating deterrence unlikely to work in practice [1].

2. The Cartwright Conjecture

The premise of Jason Healy's "The Cartwright Conjecture" is that there is surprisingly little evidence to show that a capabilities-based strategy of cyber deterrence has the desired effect on adversaries, and that there may in fact be evidence of the opposite [14]. Healy names the Cartwright Conjecture after a statement by General James Cartwright, USMC (ret.), about the need for the United States to acquire fearsome cyber capabilities and to ensure that adversaries are aware of them: "We've got to talk about our offensive capabilities…to make them credible so that people know there's a penalty [for attacking the United States]" [14]. Healy states that the history of cyber conflict shows that the opposite is true. Nations demonstrate or brandish capabilities by actually using them, and that in turn usually leads to other nations retaliating or developing their own capabilities [14].

If one considers the history between the United States and its four primary cyber adversaries (North Korea, Iran, China, Russia), Healy argues that demonstrating cyberattack capabilities leads to escalation and not stability [14]. North Korea is the least helpful case; the U.S. had very few cyber options to respond to North Korean malware attacks against Sony as well as their release of the WannaCry ransomware, in part because of their lack of connectivity as a society or government to exploit [11]. The case of Iran is more helpful in showing escalation; Iran's response to the alleged U.S.-Israeli attack against its nuclear program was ultimately to start developing cyber organizations and capabilities of its own. Multiple cyberattacks against critical infrastructure, such as the ones against Saudi Aramco and RasGas, are believed to have been Iran's response to Stuxnet [15]. While not much is known about U.S. operations against China, both parties feel that they are victims of each other's aggression in cyberspace. The Snowden leaks allowed China to solidify claims of being the aggrieved party [16], while incidents like the 2015 hack into the Office of Personnel Management (OPM) generated outrage on the part of many senior U.S. policymakers, who also expressed a desire to strike back as a result [17]. Finally, Healy states the heightened

aggression demonstrated by Russia in Ukraine and in the 2016 U.S. presidential election influence operations is in part driven by a need to signal to the United States that Russia is an equal in cyberconflict, potentially in response to the Snowden leaks [14].

These cases of tit-for-tat escalation lead Healy to draw several conclusions [14]. He states that because the malware used for penetrating the U.S. electrical grid had been in use for several years, it may not necessarily be the case that all cyber capabilities are one-time use weapons. If facilities or networks do not have the proper manning, training, or equipment to quickly adapt to new forms of malware, the shelf-life or reusability of cyberweapons may be extended [14]. Additionally, adversaries in cyberspace seem to demonstrate their capabilities by employing them against real-world targets, rather than using a controlled environment or actually talking about them [14]. Finally, interaction among adversaries in cyberspace seems to be characterized by persistent contact below the threshold of armed conflict [14]. In light of this, Healy concludes that a strategy of persistent engagement with adversaries and defending forward in order to control key "terrain" in cyberspace may be a better strategy than attempting to achieve deterrence. There are still dangers to be avoided using this strategy, such as the danger of forsaking the vision the United States elevates of the Internet as a peaceful global commons, or that the dangers of escalation are still present; but it may be the least bad option available to policymakers to prevent adversaries from threatening U.S. interests in cyber space [14].

3. The Challenge of Cyber Signaling

Libicki's and Healy's works establish the baseline of challenges that need to be overcome for successful brandishing of cyber capabilities to establish credible deterrence. This thesis aims to build on this work by investigating specific possibilities of brandishing a strategic capability in cyberspace, with the intent of coercing as well as deterring an adversary. This will include a closer evaluation of the benefits and risks of doing so, utilizing historical cases studies where either successful or unsuccessful instances of signaling for coercion occurred. These cases studies provide a basis to consider whether or not cyber signaling is suitable in general for the purposes of coercion or deterrence. This study will not encompass

all of the aspects of deterrence in cyberspace, instead focusing specifically on issues directly related to the possibility of signaling in cyberspace.

D. FOCUS AND STRUCTURE OF RESEARCH

Chapter I of this paper highlighted several key issues with signaling in cyberspace. If cyber capabilities are not inherently potent enough to coerce adversaries, or if the only way to convince an adversary of a capability is to actually use it against them in manner that provokes a retaliation, or, if brandishing cyber capabilities has a negative effect on the coercive power of said capabilities, then the concept of signaling for creating deterrence is in jeopardy. The rest of the thesis is devoted to researching that question.

Chapter II consists of two sections focusing on relevant historical data that can be used to make inferences about signaling, focusing on the activities of both the United States and Russia in cyberspace. Section I consists of historical case studies of conflict in cyberspace that shed light on the escalatory nature of using cyber capabilities. Section II is a case study of the deterrence signaling at play in the 1991 Persian Gulf War, providing an illustrative non-cyber case for contrast. These historical examples of signaling for cyber deterrence and conventional deterrence will be used to shape further discussion about the viability of signaling for deterrence in cyberspace.

Chapter III will conclude the thesis with an evaluation of how the difficulties with signaling for cyber deterrence affect the debate between persistent engagement and deterrence as U.S. policy options, and the potential uses of signaling outside of deterrence. The evaluation in this research of the viability of signaling to adversaries for deterrence in cyberspace will help inform decisionmakers about the usefulness of pursuing such a strategy and help provide a framework of clear opportunities and limitations within which cyber signaling can be used to achieve strategic goals.

II. THE POSSIBILITIES OF SIGNALING FOR COERCION IN CYBERSPACE

A. INTRODUCTION

Both the U.S. and Russia have in one way or another attempted to signal adversaries for deterrence in cyberspace. The attempts at signaling may not have had signaling for coercion as their primary goal, and in some cases may have actually been accidental. However, the acts of aggression in cyberspace made by nation-states seem to usually be taken by the intended targets, as well as neutral parties, as being escalatory in nature. The Russian use of cyberspace to project power in the Estonia crisis in 2007, in Georgia in 2008, and in the U.S. presidential elections in 2016 have been viewed as aggressive actions that signal the intent and capability that Russia will use cyberspace as a means of projecting power. The same can be said of the United States: the Stuxnet attack on Iran (widely attributed to the United States and Israel); the Snowden leaks; and the recent overt signaling campaigns by CYBERCOM against ISIS and the Russia-based Internet Research Agencies all were signals to the rest of the world that the U.S. government viewed cyberspace as a 5th domain within which force could be applied, and that it was both capable and willing to fight wars in and from it.

Section I of this chapter will take a closer look at the more significant examples of notable actions in cyberspace by both Russia and the United States to determine if the signaling elements of these actions, intentional or not, had the effect of coercing adversaries in any way to the advantage of the signaler. Section II will take a close look at the signaling for coercion that occurred in the 1991 Persian Gulf War, and use this case to shed light on the elements that may be lacking in an effective strategy of cyber deterrence. The successful deterrence of Saddam Hussein from using chemical weapons, as well as the unsuccessful attempts by the coalition forces to compel him to leave Kuwait short of armed conflict, highlight necessary concepts of deterrence needed to determine if such a policy in cyberspace could be successful.

B. HISTORICAL CASE STUDIES OF CYBER SIGNALING

1. Estonia and Georgia

In 2007 Russian patriotic hackers not officially connected to the Russian government attacked Estonia's information networks. The attacks occurred in response to the Estonian government deciding to relocate a WWII-era statue of a Russian soldier, which was met with anger by many ethnic Russians in both Russia and Estonia. Christopher Wrenn describes the conflict as taking place in two phases over the course of twenty-three days [4]. The first phase consisted of low-complexity attacks that included the defacement of government websites, smaller denial-of-service attacks, and propaganda and misinformation. The second phase consisted of cyberattacks of much greater sophistication and coordination, and were characterized by DDoS attacks that targeted the backbone routers of Estonia's information infrastructure, government websites, and Estonia's banking infrastructure. The most significant attack was a DDoS attack against Estonia's largest bank, which lasted twenty-four hours and eventually caused the bank to go offline [4].

Estonia was particularly vulnerable to cyberattack because it was one of the first nations in the world to depend heavily on the Internet to conduct official business. 97 percent of Estonia's banking occurred online that year, and in the following year 88 percent of Estonians filed their taxes online [4]. The government was also heavily dependent on the internet to function: "It regularly held paperless cabinet meetings, courts and law enforcement agencies relied upon a paperless e-case system, elections were computerized, doctors depended upon a national system to review medical records, and schools used an e-school system to communicate daily assignments and grades to students and parents" [4]. Estonia prided itself on being on the forefront of information technology for its time [18]. This increased "surface area" of attack amplified the effects of the Russian attacks, and made Estonia particularly vulnerable to coercion via cyberspace. The overall effect of these attacks was the equivalent of a "cyber blockade," where internet connection throughout Estonia was severely degraded [18].

Despite its accentuated vulnerability to the Russian cyber campaign as a highly-connected country, the Estonian government was not dissuaded from relocating the statue to its intended destination in the Estonian Military Cemetery [18]. Conversely, Estonia did not retaliate against Russia with either conventional or cyber capabilities. Though Estonia is a member of NATO, the alliance did not invoke Article V of the treaty due to indecision of whether or not to classify the attacks as a use of armed force against Estonia [4]. Article V states that an "armed attack" against one member of NATO constitutes an attack against all members, and that all members shall come to aid the attacked member by all means necessary, including the use of armed force [6]. Instead, NATO invoked Article IV of the treaty, which states that members will "consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened" [6].

NATO's focus in cyberspace prior to the conflict had merely been to secure its own networks, mainly by establishing the NATO Computer Incident Response Capability in 2002 [4]. In order to address the need to adapt to defend member states in cyberspace, NATO established the Cooperative Cyber Defense Center of Excellence (CCD COE) in Tallinn, the capital of Estonia [18]. The intent of this organization was to help NATO begin to update its strategic policies to account for a cyber-attack on one of its members [4].

In sum, the use of cyber capabilities by Russia to coerce Estonia did not achieve its objective. Estonian was not coerced; it proceeded with the action (moving the statue) that had sparked the cyberattack. Instead, all the cyberattack accomplished was to signal to the world that the Russians were capable and willing to use cyberspace as a means of power projection. This demonstration failed to coerce or intimidate NATO more broadly. Conversely, through formation of the CCDCOE and other NATO planning, the Estonia attack resulted in NATO being more prepared for future Russian cyber actions against NATO than it would have been otherwise.

In August 2008, Russia invaded the Georgian province of South Ossetia in order to secure its independence from Georgia, along with the region of Abkhazia. Unlike the Estonia incident, the invasion consisted of both conventional and cyber actions [19]. Coinciding with the Russian conventional forces crossing the border into South Ossetia

were cyberattacks against Georgian IT infrastructure, which caused 35 percent of Georgia's networks to stop functioning, 60 percent of its networks to suffer decreased functionality, Georgia's cell phone infrastructure to cease working, and the National Bank of Georgia to cease operations over the course of the conflict [4], [20]. The conflict was remarkable due to the coordination between the conventional assaults and the cyberattack; the most powerful cyberattacks coincided with the first three days of the Russian ground assault into South Ossetia. The targets of the cyberattacks were primarily directed at high-level government organizations and media sites such as the Ministry of Foreign Affairs, the Parliamentary and Presidential websites, the largest online forum, and both the Association Press and the largest English-speaking Georgian news page, all in order to prevent Georgia from communicating internally with its people as well as the outside world [4], [19]. The conflict ended with both Abkhazia and South Ossetia outside of Georgian political control and being recognized as independent territories by Russia [4].

Georgia did retaliate against Russia in cyberspace by taking actions against two Russian news media outlets, though they did not cause any lasting impact and were quickly reversed [4]. In retrospect, neither Georgia nor Russia viewed the role of cyberspace as having significant impact on the outcome of the conflict. According to Capt. Sarah White, U.S. Army, interviews with members of the Georgian military and government revealed that they believed the cyberattacks had minimal impact on the overall outcome of the conflict: "While the cyberattacks added a layer of chaos to the Georgian response, they did not affect the military decision making about the crisis in a significant way" [20]. Part of this is likely due to the fact that Georgia as a society was not nearly as integrated into the Internet as Estonia; its population only had 7 Internet users per 100 people in 2008, compared to Estonia's population having 57 Internet users per 100 people, in 2007 [4]. The Russians also took a dim view of the effectiveness of their cyber operations in the conflict: "Internal appraisals of the Russian military's performance uncovered a number of operational deficiencies, not least of which was the failure of the cyberattacks, and the broader information campaign in which they were nested, to successfully control the war's narrative" [21].

Therefore, the coercive power of cyberattacks against IT infrastructure would not have been sufficient by itself to compel the Georgians to cede South Ossetia and Abkhazia. More broadly, as in the Estonia case, the cyberattacks did more to alert Russian adversaries of the need for preparation for future Russian aggression than to intimidate Russian adversaries into more Russia-friendly behavior.

The conflicts in Estonia and Georgia are not true examples of signaling for coercion on either side. Coercion requires an explicit threat made, prior to the outbreak of hostilities, of the threatened use of force in order to change the behavior of the target. Russia did not overtly threaten either Estonia or Georgia beforehand with the use of either cyber capabilities or a conventional assault. The Russian government has never admitted to involvement in the Estonia attacks; it is only by looking at the evidence of relationships between the patriotic hackers and government officials, as well as the sophistication of the second phase of the attacks, that most have come to the conclusion that the government was involved in the attack [4]. While the identity of the attackers in the Georgia conflict are obvious, in that case there was no explicit brandishing on the part of Russia prior to attacking in order to compel Georgia to cede Abkhazia or South Ossetia. Neither did Estonia or Georgia have established thresholds of aggression in cyberspace that clearly signaled to Russia that they would be retaliated against should they cross those thresholds.

These two conflicts did, however, signal to the world that Russia viewed cyberspace as "an object of contestation and as a vector for generating strategic effects and outcomes" [19]. It seems no coincidence that by 2010, several nations had begun to stand up organizations and policies that enabled more coordination of military cyber capabilities. NATO's establishment of the CCD COE has already been mentioned. On November 12th, 2008, U.S. Secretary of Defense Robert Gates directed the formation of U.S. Cyber Command as a sub-unified command under USSTRATCOM; the command achieved initial operational capability on May 21, 2010 [22]. Talks to merge existing military cyber commands started in February 2008, and then "began in earnest that summer," right around the timeframe of the Georgia-Russia conflict. In summer of 2009 the United Kingdom began the formation of the Office of Cyber-Security of the Cabinet Office, with the mission of coordinating policy in cyberspace for the whole government; and the Cyber-Security

Operations Centre, with the mission of combining resources and expertise in both the private and government sector [23]. In 2010 the South Korean defense ministry announced a cyberwarfare command center to combat attacks on their military and government networks [23], [24]. In 2008, India began increasing its cybersecurity workforce by 15,000 personnel, tasked the Indian Army Cyber-Security Establishment with conducting audits within the military, and established a Computer Emergency Response Team (CERT) in 2009 with the help of the U.S. CERT [23]. To be thorough, India and South Korea began their initiatives partly in response to Chinese intrusions into their networks [24], representing still another case that reinforces the trend of escalation of defense preparations in response to increasing adversarial displays of cyberattack capabilities.

The cyber capabilities displayed in the two conflicts did not achieve their immediate objectives. Rather, many states saw in these instances the potential dangers as well as benefits of cyberspace being used to achieve strategic, operational, and tactical military or geopolitical ends, and began to develop their own cyber capabilities in order to meet those goals. In these cases, the only signaling achieved by the attackers was to spur the defenders to better preparation for future attacks.

2. Stuxnet

The Stuxnet attack on Iran was the first cyberattack to cause physical destruction against a target [13]. According to the famous David E. Sanger New York Times article, which supposedly received its information from a high-level U.S. government official, the initial intent of Stuxnet was to clandestinely attack the Iranian uranium enrichment facilities at Natanz in order to disrupt their nuclear weapons program. It was deployed in 2008, and remained active until 2010 when it was accidentally discovered [13]. In order to be successful Stuxnet needed four zero-day vulnerabilities, the certificates from two well-standing software companies so that malware would be recognized as valid software, and also the exploitation of the PLC's (Programmable Logic Controllers) that were used by the Iranian enrichment facilities [7], [25]. Any one of these vulnerabilities being patched may have resulted in the malware being unable to fulfill its purpose. In addition, according to the Sanger article, the attack required months to gain the sufficient knowledge of the layout

of the Natanz facility, the right equipment to adequately test the worm, and finally the placement and access of human agents to insert the malware [13]. Some estimates project that the attack was able to set back Iran's nuclear weapons program by as much as 18 months [13].

The initial intent for Stuxnet seems to have been to remain clandestine in nature; it was specifically programmed to tell the operators in Natanz that nothing was wrong with the equipment, and remained hidden for two years prior to being discovered. Stuxnet ultimately spilled onto the Internet due to a coding error in a later iteration of the malware, which compromised both the malware as well as (allegedly) the identity of the attackers [13]. Many came to the conclusion that the only actors with the skill, resources, and motive to attempt such an attack were the United States and Israel. This accidental spillage onto the Internet may account for the anonymous leaks in the Sanger article: the goal of the leaks may have been to repurpose the attack as a means of brandishing cyber capabilities to Iran as well as the rest of the world. Potentially, the Obama administration made the best they could of the situation and repurposed the Stuxnet worm into a form of brandishing or signaling. Whether intended or not, this repurposing of Stuxnet to brandish cyber capabilities has effectively signaled to the world in a powerful way the capabilities of the United States and Israel. No one who believes that the United States and Israel conducted the attack can doubt that both are among the most advanced cyber actors in the world, capable and willing to use highly sophisticated malware to cause damage to adversary critical infrastructure.

However, if the goal of this brandishing was to coerce or persuade Iran to give up its nuclear weapons development, it failed to do so [26]. Also, the Stuxnet attack apparently has instead encouraged Iran to develop and use its own cyber capabilities against targets of a similar nature. Soon after the attack was discovered, Iran announced that it would spend around $1 billion on developing a cyber warfighting unit [7]. A string of attacks on Western infrastructure following the Stuxnet attack were attributed to Iran, including the Shamoon attack on the Saudi Aramco oil company in 2013–2014 that forced 30,000 computers to go offline, the hacking of the Las Vegas Sands Corporation, and the DDoS (Distributed Denial of Service) attacks on U.S. banks [15], [7]. Some analysts judged that Iran's primary

motive was a revenge response to the Stuxnet incursion, rather than an effort to demonstrate capabilities for future coercion or revenge [15].

3. Edward Snowden

The fallout caused by the Edward Snowden breach in the summer of 2013 was, ironically, a form of brandishing capabilities in cyberspace. In June 2013, Edward Snowden leaked millions of documents to the world that detailed both the capabilities and past activities of the National Security Agency to the world [7]. The leaks demonstrated that the United States National Security Agency had the skill to infiltrate many systems thought to be secure. Although this was by no means intentional on the part of the government, it did have the impact of signaling to the world at large the fearsome capabilities of the United States in cyberspace, as well as provide in detail the actual employment of those capabilities against a variety of targets. In the words of Henry Farrell in a Washington Post article, "Snowden's revelations may provide a much more credible signal about the strength of the U.S. cybersecurity apparatus than anything that the government itself could say" [27]. The fact that Snowden conducted the leaks as a protest against the NSA gave much more credibility to the United States' capabilities in cyberspace [27].

The unintentional nature of this "brandishing" means that there was no direct communication with an adversary about thresholds of behavior and specified punishments. This lack of intentional communication with a specified target means that this does not necessarily qualify as an instance of signaling for deterrence. The prospect is whether the Snowden leaks brandished capabilities in a way that would intimidate generally or support future specific deterrence or coercion threats.

Relating to that prospect, these leaks to do not seem to have resulted in a decrease in adversarial cyberspace activity; they may have even caused an increase in escalation. Several nations played the victim following the incident, most notably China [28]. A commentary in an official Chinese news agency, the Xinhua News Agency, stated: "The United States, which has long been trying to play the innocent victim of cyberattacks, has turned out to be the biggest villain in our age" [16]. The Chinese are attributed by the

intelligence community with multiple instances of intellectual property theft even after the Snowden revelations; examples include the breach into the Office of Personnel Management in 2014 and 2015 that stole the sensitive data of 21 million Americans with security clearances, the 2017 Equifax breach that stole the personal information of 145 million Americans, and the 2018 data breach into Marriott International which compromised the personal data on hundreds of millions of accounts [3]. Russia was certainly not deterred or intimidated, as in late 2014 they instigated a civil war in Ukraine, and in 2015 were attributed with the Black Energy malware attack on the Ukrainian power grid that disrupted the power of millions in Ukraine. Other attacks following Snowden include the 2017 NotPetya ransomware attacks [3].

It is difficult to attribute specific attacks that occurred to a reaction against the Snowden revelations. But the fact that adversarial activity continued unabated following the leaks speaks to the impotence of such signaling, despite the credibility of the source, in terms of general intimidation effects.

4. BlackEnergy

The BlackEnergy attack was a significant escalation of the use of cyber capabilities in the Ukraine conflict in the winter of 2015. When pro-Russian president of Ukraine Viktor Yanukovich was forced to flee Ukraine, Russia promptly annexed the Crimean Peninsula and instigated civil war in the eastern Ukrainian provinces of Donetsk and Luhansk with the intention of having them breakaway from Ukraine. Russia's use of cyber capabilities prior to the use of BlackEnergy were limited to supporting information warfare objectives [18]. Their primary goal for a time was to use cyber warfare to cause the Ukrainian populace to doubt the credibility and legitimacy of the government. Other uses involved sending text messages to Ukrainian soldiers encouraging them to defect [29].

The BlackEnergy incident caused a power outage for over 220,000 residents in western Ukraine, and is attributed to pro-Russian actors trying to signal displeasure with Ukraine over anti-Russian policies [30]. It was a malware package first discovered in 2007, but updated in 2014 to add new capabilities [31]. While some of the capabilities embedded in the malware were very advanced, the three distribution centers were compromised by

vulnerabilities in Microsoft Office documents, a relatively simple tactic. This constitutes the first and only confirmed instance of a cyberattack that brought down an electrical power grid [31]. The power in the affected regions was only out for a span of 1–6 hours, even though some forensics analysts believed the attackers could have permanently taken the stations offline. The fact that effects of this attack were not nearly as wide-spread as they could have been speaks to both the sophistication of the hackers and the possible intent to signal to Ukraine displeasure over the nationalization of power companies owned by Russian businessmen [18], although this is based on circumstantial evidence. If this is the case, it would one of the very few instances of intentional signaling in cyberspace by brandishing sophisticated cyber capabilities.

The escalatory responses to this attack are uncertain. The fact that Ukraine was already embroiled in a civil war with Russian-backed separatists likely made the impact of this escalatory move in Ukraine less meaningful. While this may have been a covert instance of signaling to Ukraine, the prescribed response desired from Ukraine was not evident from the attack alone.

5. 2016 U.S. Presidential Election

The influence operations attributed to Russian hackers in the 2016 U.S. presidential elections demonstrated the willingness and fearsome proficiency of the Russians to use cyberspace to achieve their strategic goals. It is now known that in the months leading up the election, the Democratic National Convention's computer networks had been the target of multiple hacks, and tens of thousands of sensitive documents and emails belonging to the senior Democratic Party officials were released onto the websites WikiLeaks and DCLeaks [32], [33]. An entity named Guccifer 2.0 claimed responsibility for the hacks, which was later assessed by the Office of the Director of National Intelligence (ODNI) to be the GRU, Russia's Main Intelligence Directorate [33]. ODNI's report assessed that President Vladimir Putin had ordered the influence campaign against the United States with the overall objectives to "undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency" [33]. While the attacks did not display a fearsome capability to impact critical infrastructure or secure IT

networks, they did show that Russia had become very proficient at using cyberspace as a vector for information operations to influence the domestic politics of other nations.

Whether this was an instance of signaling on the part of Russia targeting the United States is another matter. The ODNI assessed that the motive for the Russians' influence operation was mainly to put a more "Russia-friendly" candidate in the White House; Secretary Hillary Clinton had made statements in the past that were considered by President Putin to be inflammatory and anti-Russian. There was no mention of signaling for threatening for coercive purposes. Information operations and influencing foreign domestic politics is a long-standing tactic of the Russians [33]. There may have been an implicit "threshold" that was conveyed to the United States, in that Putin stated that the United States was conducting influence operations in Russia. If so, then this may have been an implied threat to the United States of the consequences of U.S. actions. However, the United States certainly responded to it as a threat against the integrity of its electoral system.

The U.S. initial response to this attack was limited to sanctions [34]. It came to light later that, though the Obama administration debated retaliating quickly, the fact that the U.S. stood more to lose from a cyber conflict with Russia, as well as fears of Russia causing havoc with the power grid, mitigated the response [34]. Jason Healy describes this as the only case of where the Cartwright Conjecture worked, in that a crushing U.S. response was deterred by the threat of further Russian cyberattacks [14]. However, subsequent events indicate that that conclusion is not the full story. The incident resulted in the changing of the U.S. cyber doctrine to one of persistent engagement. The 2018 Department of Defense Cyber Strategy adopted a strategy that seeks to create cyber security through, among other things, persistently contesting malicious activity in cyberspace through day-to-day competition, reinforcing norms of responsible state behavior in cyberspace, and adopting a stance defending forward in order to shape cyberspace to the advantage of the U.S. [35]. Rather than having a stance characterized by holding devastating cyber capabilities in reserve to be used as a threat, the U.S. adopted a view of cyberspace as one of constant friction with adversaries. This change in policy was also accompanied by an increased willingness to publicize recent or even ongoing U.S. cyber operations against Russia. A

more in-depth discussion of this strategy takes place in Chapter III. Here, the point is that, in the long run, rather than being intimidated by demonstrated Russian cyber capabilities, the United States reacted by bolstering its own capabilities, posture, and activities.

6. U.S. CYBERCOM Campaign

In February 2019, anonymous U.S. officials leaked to the media that USCYBERCOM conducted an offensive cyber operation against the St. Petersburg-based Internet Research Agency, a Russian troll-farm that was implicated in the 2016 influence operation [36]. This was officially confirmed in July 2020 in an interview with the Washington Post by President Trump [37]. In September 2019, NPR released a story from General Nakasone, the current commander of CYBERCOM, that went into unprecedented detail about the counter-ISIS campaign named Operation Glowing Symphony conducted by Joint Task Force ARES, the unit formed by CYBERCOM for that specific mission set. Even though the events mentioned in the article occurred in 2016, General Nakasone released the story three years later with the seeming intent of signaling to Russia that a similar group was tasked with a similar mission targeted at them.

The article finishes with briefly mentioning a similar effort concerning Russia: “All this is important because you can draw a straight line from Joint Task Force ARES to a new unit from the NSA and U.S. Cyber Command: something called the Russia Small Group. Just as Joint Task Force ARES focused on ISIS, the Russia Small Group is organized in much the same way around Russian cyberattacks” [38]. In the article, Nakasone mentions that his first act upon assuming command was to assess Russian interference in the elections, leaving the reader to conclude that his openness about mentioning the Russian Small Group was a way to signal that U.S. Cyber Command was actively ramping up its efforts to combat Russia in cyberspace to prevent another occurrence [38]. Finally, in August 2020 General Nakasone co-authored with Michael Sulmeyer a Foreign Affairs article about competing in cyberspace via a strategy of persistence and defending forward [39]. The article opened with an account of personnel from Cyber Command deploying to Montenegro to combat Russian interference in that

country, and its purpose was to demonstrate how the U.S. was successfully adhering to its new strategy in cyberspace.

This series of public releases about specific U.S. cyber operations speaks to a new willingness on the part of General Nakasone to overtly signal to adversaries, Russia in particular, U.S. willingness and ability to use cyber capabilities against Russia in a much more aggressive way. This response to the Russian influence operation is the only instance of intentional, overt signaling for deterrence to an adversary that the researcher has discovered. Though this new stance of publicity may be in part meant for the American public in order to assure them that the Russian cyber threat is not being overlooked, it still remains an instance of overt signaling targeted against a threat in cyberspace. Yet, even in this case, the signaling is general and not directed against a specific Russian action to be deterred. It is too soon to see the potential results of such signaling. Because this brandishing was done within the framework of persistent engagement, which assumes the inevitability of conflict in cyberspace below the threshold of actual war, it is unlikely that policymakers expect it to be successful in the short term [40].

7. Cyber Signaling Case Record

Table 1 summarizes the findings in the preceding case studies, in terms of whether a signal was sent by demonstrating cyber capabilities, whether that signal succeeded in coercing the target state, and whether the impact was ultimately escalatory.

Table 1. Responses to Cyber Attacks

	Was there a signal sent?	Did it coerce adversary?	Did escalation occur?
Estonia	No	No	Yes
Georgia	No	No	Yes
Snowden	No	No	Probably
BlackEnergy	Possible	No	Unknown
2016 Election	No	Short-term: Yes Long-term: No	Yes
CYBERCOM campaign	Yes	Unknown	Unknown

The only confirmed instance(s) of signaling has occurred too recently to determine whether or not it resulted in escalation or deterrence. However, it seems that the use of cyber capabilities trends toward escalation, and that cyber capabilities are not capable of posing a large enough threat to deter an adversary.

C. 1991 PERSIAN GULF WAR

In order to properly frame the concept of signaling for the purposes of coercion in cyberspace, this section briefly showcases a conventional scenario of capability signaling. The 1991 Persian Gulf War provides a relatively recent example of signaling for deterrence.

In late 1990, Saddam Hussein invaded Kuwait for the purposes of taking control of the oil fields located in that country. During the planning and preparation by the Bush Administration to retaliate by military force and drive Saddam out of Kuwait, there was much debate about how to address the possibility that Saddam and the Iraqi military might use chemical weapons against coalition military forces. On 24 December, 1990, President Bush and his advisors discussed at Camp David the possibility of threatening the Saddam Hussein regime with the use of nuclear weapons in response to any employment of chemical or biological weapons [41]. Several senior political and military leaders had overtly suggested the use of nuclear weapons in retaliation. General Norman Schwarzkopf recommended to the Joint Chiefs of Staff that the U.S. send an overt threat to the Iraqi regime [41]. However, at Camp David the idea of both an overt threat of nuclear weapons, as well as the idea of actually using them, was rejected by President Bush. The deterrence factor that President Bush had in mind was an ambiguous threat to both Saddam and the Ba'ath Party that did not necessarily preclude the use of nuclear weapons, but did not overtly commit them as a response. In their joint memoirs, George H.W. Bush and his National Security Advisor Brent Scowcroft recall this particular issue:

> What if Iraq decided to use chemical weapons? We had discussed this at our December 24 meeting at Camp David and had ruled out our use of them, but if Iraq resorted to them, we would say that our reaction to them would depend on circumstances and that we would hold divisional commanders responsible for them and bring them to justice for war crimes. No one advanced the notion of using nuclear weapons, and the President rejected it

> even in retaliation for chemical and biological attacks. We deliberately avoided spoken or unspoken threats to use them on the grounds that it is bad practice to threaten something you have no intention of carrying out. Publicly, we left the matter ambiguous. There was no point in undermining the deterrence it might be offering. [42]

The Secretary of State at the time, James Baker, also records his version of the meeting. The additional element of deterrence that was added in was to deliberately threaten the Ba'ath regime with retribution if they used chemical weapons. In his memoirs, he writes:

> The President had decided, at Camp David that December, that the best deterrent to the use of weapons of mass destruction by Iraq would be a threat to go after the Ba'ath regime itself. He had decided that the U.S. forces would not retaliate with chemical or nuclear weapons if the Iraqis attacked with chemical munitions. There was obviously no reason to inform them of this. [43]

In his letter to Saddam Hussein, it is evident that President Bush followed this strategy in threatening the regime, but without specifying how the U.S. would respond. He wrote:

> The United States will not tolerate the use of chemical or biological weapons or the destruction of Kuwait's oil fields and installations. Further, you will be held directly responsible for terrorist actions against any member of the coalition. The American people would demand the strongest possible response. You and your country will pay a terrible price if you order unconscionable actions of this sort. [41]

Secretary Baker also met with the Iraqi Foreign Minister at the time, with the intent of impressing upon the Iraqi regime the resolve of the U.S. government to punish the use of weapons of mass destruction, but without specifying how they would do so. The threat of nuclear weapons was meant to be implied so that the U.S. would not lose credibility by making an idle threat, but the question of their possible use still causing Iraqi decisionmakers to be afraid of approaching that line:

> If the conflict starts, God forbid, and chemical or biological weapons are used against our forces, the American people would demand vengeance. We have the means to exact it. With regard to this part of my presentation, this is not a threat, it is a promise. If there is any use of weapons like that, our objective won't only be the liberation of Kuwait, but also the elimination of the current Iraqi regime, and anyone responsible for using those weapons would be held accountable. [43]

Another factor that must be taken into account is the fact that several U.S. leaders at the time were more overt in public about the potential use of nuclear weapons in retaliation for any Iraqi use of WMD's. General Schwarzkopf is already mentioned as having recommended the use of nuclear weapons. At a press conference in January 1991, he said: "If Saddam Hussein chooses to use weapons of mass destruction, then the rules of this campaign would probably change – and I think that's as it should be" [41]. Lt. Gen. Walter Boomer, who was the senior Marine commander in the region, said at a press conference in response to a question about responding to Iraqi WMD's, said the U.S. response would be "something worse, something terrible" [41]. Then Secretary of Defense Dick Cheney brought up a different possible response, in that Israel might retaliate with nuclear weapons if Saddam went too far: "I assume he [Saddam Hussein] knows that if he were to resort to chemical weapons that that would be an escalation to weapons of mass destruction, and that the possibility would then exist, certainly, with respect to the Israelis, for example, that they might retaliate with unconventional weapons as well" [41].

There is ample, though not irrefutable, evidence that this effort at signaling by the Bush Administration had its intended effect. Obvious (though not conclusive) proof is that the Iraqis never did use chemical weapons. However, the postwar statements by senior Iraqi leaders indicate that the potential use of nuclear weapons weighed heavily on the mind of Saddam Hussein, and as a result neither chemical nor biological weapons were ever used. The head of Iraqi military intelligence affirmed this later:

> We told him (Saddam) very clearly that should he use chemical weapons they [the Americans] will use their nuclear weapons. I do not think Saddam was capable of taking a decision to use chemical weapons or biological weapons, or any other type of weapons against the allied troops, because the warning was quite severe and quite effective. The allied troops were certain to use nuclear arms and the price will be too high and dear. [41]

When the UN Special Commission later inspected the WMD arsenal of Iraq in order to hold officials accountable, those officials stated that the nuclear threat by the Bush administration was the primary reason that the weapons were never used [41]. The head of the UN Commission, Rolf Ekeus, stated that "Iraqi officials claimed they decided not to use the weapons after receiving a strong but ambiguously worded warning from the Bush

administration on January 9, 1991, that any use of unconventional warfare would provoke a devastating response" [41].

The statements made by Iraqi military officials strongly support the conjecture that the implied threat of nuclear deterrence worked. An interesting question would be if an explicitly worded threat would have made a difference. This would depend on public reaction to the administration making such a statement; though several decisionmakers had displayed support of using nuclear weapons, if there was a large enough outcry by the American public and the world against their use, it may have tempted Saddam to call the bluff of President Bush, because the political backlash of using such weapons may have caused him to back off. This still would not have saved Saddam's regime in the end, as the coalition would still have dismantled his regime, but it would have also damaged the credibility of the United States on the world stage. In this scenario, the implied threat was a safer move on the part of the Bush Administration, as long as the promise to depose Saddam was overt.

Obvious but important to this discussion is the fact that Iraqi leaders had no doubt of the ability of the United States to employ nuclear weapons. This prior knowledge may cast doubt on whether or not the signaling on the part of the United States actually made a difference in the outcome. It may be that the very existence of nuclear weapons, regardless of whether or not the United States threatened to use them or not (overtly or otherwise) may have had an impact on the decision of Iraq to not use chemical weapons. This concept, labeled existential deterrence [44], may have been the sole reason that the Iraqis chose not to escalate with weapons of mass destruction, as it would have given the coalition a reason to respond in kind.

However, it is clear that this type of deterrence was not at work in the calculus of Saddam Hussein in the initial choice to invade Kuwait. It is largely believed that Saddam chose to invade Kuwait in order assert Iraq's historical claim on Kuwait and establish control of a large part of the Gulf's oil-production [45]. This can be attributed to either a failure of U.S. diplomatic signaling, Saddam's economic need for more stake in the Gulf's oil production, the desire for more political and economic power in the region, or some combination of all three. However, what is evident is that the subsequent attempt by the

international coalition to compel Saddam to withdraw did not work. The repositioning of massive amounts of U.S. forces to the Gulf and the Saudi border, UN resolutions, and the efforts of French, Arab, and Soviet mediators to allow Saddam a peaceful way out were all unsuccessful as instruments of coercion. Janice Stein concluded that based on Saddam's political and economic goals, and his belief that he could cause enough casualties against the coalition expeditionary force to make such a campaign politically untenable for the Bush Administration, the Gulf War was inevitable [45]. Saddam's fear of a nuclear response to invading Kuwait was not a factor in his calculus.

This historical case of deterrence offers a sound framework by which to analyze a successful attempt to signal to an adversary the intent to use a devastating capability in order to change their behavior. The Bush administration wanted to deter the Iraqis from using chemical and biological weapons. They had the capability, both conventional and nuclear, to impose devastating costs on both the Iraqi military and the Ba'ath Party regime in Baghdad. Using nuclear weapons was not an option that the President wanted to consider, but the Iraqis were not aware of that. Even had the President declared nuclear weapons off the table, it is questionable whether the Iraqis would have believed it. The United States and the coalition had the conventional capabilities to remove the Saddam regime from power, but unlike the nuclear capability, were actually willing to use conventional weapons should they be needed. The letter from the President to Saddam, as well as the discussion that Secretary Baker had with the Iraqi Foreign Minister, were strongly but ambiguously worded as to not commit the U.S. to nuclear weapons should Iraq cross the line, but certainly suggesting their use if they did. The public statements by other senior U.S. leaders expressing more overtly the possibility of using them, in conjunction with the fact that coalition forces were mobilizing in great numbers to the Iraqi border, gave considerable weight to the threats of President Bush. The combination of strongly-worded public overtures by U.S. leadership, the established capability of the U.S. to use nuclear weapons, and the deployment of conventional military assets enabled the United States to effectively convince or signal to Iraq both the capability and intent to use nuclear weapons as well as depose the Ba'ath regime from power, should the Iraqis decide to cross the line of using WMD.

On the other hand, existential deterrence did not seem to be a factor in Saddam's calculus for invading Kuwait in the first place. It is not provable whether this form of deterrence was active in Saddam's decision to not use chemical or biological weapons, but research seems to show that the implied threats by the United States had an effect that prevented further escalation of the conflict with the use of WMD.

D. CONCLUSION

In the Gulf War case study, the major "ingredients" for successful deterrence signaling in this case were an established capability in the eyes of the adversary for the deterrer to impose costs, as well as the credibility of the Bush administration. As mentioned before, at this point in history no one doubted the capability of the United States employ nuclear weapons to devastating effect, based on the many years of Mayday parades, missile testing, and nuclear detonations seen during the many decades of the Cold War. There was no need to bluff to the Iraqis about the United States' capability to attribute chemical or biological weapons usage to Iraq, or about the ability the Bush Administration had to completely destroy them, because the adversary was already convinced of the ability of the United States' ability to do both of those. The factor at issue was convincing Saddam that the United States would go to those lengths, should they cross certain thresholds of force. The need to establish credibility was the deciding factor in this attempt at signaling for deterrence, because there was no need to remind the world about the power of nuclear weapons. In the context of coercion, high credibility is contingent on having an established capability to inflict unacceptable costs upon the adversary.

While the relative importance of capability and credibility remains the same, how a state can achieve both in cyberwarfare is significantly different. A major concept shift from nuclear deterrence to cyber deterrence in this case is that credibility seems to be most readily established by the actual employment of cyber capabilities against real-world targets. Talking generically about cyber capabilities is insufficient, because it is very easy for a nation-state to claim the ability to hack into an adversary system if they have no intention of using those capabilities. Revealing the exact vulnerabilities could actually persuade an adversary of their weakness, but that would only last as long as the adversary

takes to find a sufficient patch. The historical case studies of cyber warfare leave little room for doubt concerning the credibility and willingness of most states who have cyber capabilities at this point, if only because malware and cyberweapons have been employed by multiple states consistently against a wide variety of targets.

Credibility and capability go hand-in-hand in this relatively new domain of warfare. Effectively signaling for both is possible, but can only be achieved by using such capabilities against real targets in unmistakable ways. But this, in turn, raises the question of how such signals are received by adversaries. The case studies of this chapter suggest that when cyber capabilities are brandished by actual use, rather than bolstering deterrence or coercion threats the main result is to escalate adversarial reaction.

It would be a stretch to claim that using cyber capabilities are the sole reason for the escalation seen in the case studies in the first part of this chapter. For example, the official reason given for the establishment of USCYBERCOM was intended to ensure that the U.S. Air Force would not exclusively own the cyberspace mission set, and its creation may have been part of an inevitable trend toward creating organizations devoted to securing friendly cyber space [22], [46]. Ironically, General Nakasone, the current commander of USCYBERCOM, also admitted that a 2008 attack on the Department of Defense's classified and unclassified networks also proved to be a major driver toward his command's creation [39]. It also may be that this trend is inevitable, based on the usefulness of cyberspace for espionage and information operations in the pursuit of national strategic goals.

However, it also seems to the researcher that Libicki's prediction of a cyber arms race being unlikely was too optimistic [1]. The previous case studies point to a trend in the militarization of cyberspace by the development of national organizations and policies, as well as the willingness to use cyber capabilities to achieve strategic goals. Jason Healy's assertion that Russian intrusions into the U.S. power grid deterred the U.S. from retaliating for the 2016 influence operation was made before USCYBERCOM publicly acknowledge its attack on the IRA troll farm [14], [37], and before the U.S. resorted to a policy of persistent engagement [35]. While it may be the case that there has only been one confirmed instance of intentional signaling for deterrence, it seems that the very act of

using cyber capabilities against adversaries is inferred by other nations, especially those who perceive themselves as the target, as a threat or signal that they are vulnerable to attack in cyberspace. This in turn leads to the development and use of cyber capabilities by those adversaries.

Finally, the failure of the United States and the coalition to compel Saddam to withdraw from Kuwait bears noting. The combination of the deployment of vast amounts of combat power to the Saudi-Kuwaiti border and the multiple instances of diplomatic overtures to provide the Hussein regime a way out of conflict all failed in their efforts to coerce a withdrawal. Saddam was convinced that he could mount a stiff enough resistance, and both he and coalition analysts underestimated the overwhelming advantage that modern airpower would provide in a conventional conflict [45]. Coercion using conventional military means, even when the advantage in combat power is clear, still proves problematic when the adversary is convinced that it can absorb the potential losses. The only form of coercion that was successful was the implied threat of nuclear weapons use in response to use of weapons considered to also be in that same category. But this coercion was deterrence of an Iraqi action not yet taken (use of WMD), as opposed to compellence to take a new action (withdraw from Kuwait).

Taken together, the evidence of these case studies suggests that if cyber capabilities cannot scale to the destructive capacity of either strategic or conventional weapons, deterrence relying solely on cyber capabilities is likely to prove untenable, regardless of whether one can successfully signal to an adversary resolve or credibility. This result is in large part due to the difficulty of signaling the existence of cyber capabilities, and the willingness to use them, in ways other than actually using them, which tends to produce escalation rather than deterrence.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CYBERSPACE SIGNALING FINDINGS

A. SIGNALING IN CYBERSPACE: AN EVALUATION

Signaling to an adversary that you can attribute any attack to them, that you can hold their targets at risk, and that you can do so repeatedly are all needed to provide a foundation for deterrence. Applying these three criteria to signaling in cyberspace, it is the ability to signal to an opponent that one can hold a target at risk that most falls short for cyber deterrence. It is possible to signal an adversary for all three in cyberspace. However, the core message of coercion relies upon a threat of punishment, and most cyber capabilities lack the ability to sufficiently punish or hurt adversaries. Moreover, brandishing capabilities in cyberspace is typically only possible through operational usage, which will not result in stable deterrence, only escalation. This section discusses each of these elements in light of the case study findings of the previous chapter.

Attribution, while requiring skill, is less of an issue than commonly thought. Advances in attribution, as well as established patterns of behavior over time, make it far more difficult for nations to deny malicious activity than in the past. The concept of the Advanced Persistent Threat (APT) groups, the identification of sophisticated hacker groups by the use of tactics, techniques, and procedures (TTP), has made it far more difficult for adversaries that persistently act in cyberspace maliciously to obfuscate their identity or activity [47]. The cybersecurity company Fireeye has identified over forty different hacking entities associated with five nation-states that allow for quick identification of and response to adversary penetration of networks [48]. The cybersecurity community has identified two groups, APT28 (known also as Fancy Bear and Sofacy) and APT29 (known as Cozy Bear), as being associated with the Russian Main Intelligence Directorate (GRU). These two groups have been associated with multiple attacks on U.S. cyberspace, including the 2016 attacks on the Democratic National Convention (DNC) [18]. While the level of anonymity in cyberspace varies with the type of operation being conducted (espionage vice network disruption), malicious activity over time makes it much easier to attribute threat groups.

The 2007 Estonia conflict, reviewed in the previous chapter, is a case in point. This case is often used to highlight difficulties associated with attribution due to the fact the hackers were non-government patriotic hackers, and that evidence connecting them to the Kremlin was too scarce [4]. However, as Christopher Wrenn's study shows, it is indeed possible to link the patriotic hackers to actors within the Russian government at the time, based on statements made by members of the group as well as the sophistication of the attacks in phase II [4].

The relative ease of attribution underscores the shortcomings of the other criteria for cyber deterrence. The case studies of Chapter II show that nations do not struggle with the question of who attacked them; but an expectation of attribution is not enough to deter them from doing so. Attribution of Russian responsibility in several of the early cases in Chapter II clearly did not deter Russia from its 2016 election interference efforts. Consider the Stuxnet case; even before the Sanger article came out, most of the world concluded that the United States and Israel were behind the attacks simply because no one else had the motive or skill to execute an attack of that sophistication [9]. Yet there is no evidence that this imputed attribution deterred later U.S. operations. If successful attribution of highly advanced cyberattacks is at least a distinct possibility, and yet still adversaries engage in them, it is unlikely that attempting to signal an ability to quickly attribute a cyberattack will much affect the calculus of an adversary.

There may even be a trend toward wanting to be attributed for certain actions in cyberspace. As discussed in the Chapter II case study, the U.S. might have used the Stuxnet exposure as an opportunity for brandishing. The U.S. responses to the 2016 elections seem to display a desire on the part of USCYBERCOM to be attributed for certain military actions in cyberspace. Chapter II describes General Nakasone's and President Trump's official statements affirming the U.S. military actions in cyberspace against ISIS and Russia. These instances seem to be the first attempt at overt signaling of U.S. capability and intent in cyberspace. This is consistent with the concept of deterrence, as self-attribution is necessary to be absolutely clear to the attacker what the deterring party is capable of.

The idea that it is difficult to continuously hold targets at risk holds some weight, but it also is not insurmountable. The Black Energy attack on Ukrainian power grids in 2015 proves that even complex critical infrastructure attacks can be reused if the system administrators are not able to stay ahead of malware development and techniques, and that malware can be updated to adjust to new obstacles. And even organizations that have cybersecurity as a high priority may not be able to overcome the limitations of manpower shortage. In 2018, Cybercrime Magazine predicted that there will be 3.5 million unfilled cybersecurity positions across the industry by 2021 [49]. Other statistics that will likely make holding targets at risk much easier are the overall increase in size of the Internet: the increase in internet-connected devices from 2 billion objects in 2006 to 200 billion by 2020, the need to protect 300 billion passwords around the world in 2020, and the creation of over 111 billion lines of code each year [49]. The Solarium Report details that there are "33,000 unfilled cybersecurity positions in the U.S. government and 500,000 unfilled positions throughout the United States" [3]. The manpower shortage combined with the increasing attack surface of the Internet makes it much less difficult to find multiple avenues of attack. As demonstrated by Stuxnet, air-gapped systems (which are completely isolated from the Internet) are not invulnerable if the adversary has human placement and access. Drones also could also be considered a viable way to potentially overcome this barrier [50]. A determined adversary could find multiple vulnerabilities within a single target and maintain access to that target despite a series of attempts to deny them access. Repeatedly penetrating targets, especially sensitive ones that are air-gapped, would send a credible signal to an adversary of a strong capability, and the resolve, to do so.

But signaling attribution and the ability to continuously hold targets at risk are insufficient for deterrence if there is no cyber capability that can impose a high enough cost on the adversary. The ability to hold targets at risk at all is the core issue with brandishing cyber capabilities. Up to this point in time, cyber capabilities have not demonstrated that they have sufficient coercive power, in themselves, to effectively signal for deterrence. In general, the effects of a cyberattack are temporary, difficult to repeat, and in the vast majority of cases are reversible. They cannot take or hold territory, or permanently disarm an enemy [7]. The case of Estonia gives support to this claim; despite the fact that Estonian

society was uniquely vulnerable to cyber capabilities, the Russians failed to compel them concerning the WWII statue's relocation. As Libicki points out, if the stakes in a crisis or conflict are high enough, history shows that states are willing to endure enormous amounts of punishment before capitulating to the enemy [7]. At this point in time it would be difficult to compare even an unlimited cyberwar with events such as the London Blitz in WWII, or what the citizens of Jerusalem endured in 1947 and 1948 [7], both of which failed to compel surrender.

The most damaging attacks in theory would be those conducted on financial institutions and power infrastructure. The 2020 Cyberspace Solarium report reflects on these fears in its opening theoretical scenario, and describes a Washington, D.C. that has been devastated by chemical spills due to a cyberattack on water treatment plants, massive flooding caused by malware attacks on the reservoirs, transportation accidents on the subway resulting in many casualties, and a government barely able to function without access to the Internet [3]. However, such attacks on critical infrastructure face similar barriers to the ones previously described concerning Stuxnet and BlackEnergy, which required many zero-day vulnerabilities to be successful, as well as intimate knowledge of the facilities to work; they are extremely difficult and time-intensive to pull off even once in light of the time required for reconnaissance and developing tailored capabilities. Credibly threatening such attacks when so much depends on the vulnerability of the adversary would merely provide advance warning and so cannot be a reliable foundation with which to establish deterrence.

Even if such an attack were to take place, the historical case studies show that such attacks only lead to escalation, not deterrence. Rather than being cowed into submission, nations that are on the receiving end of cyberattacks respond by developing and using cyber capabilities of their own. Cyber capabilities that cause kinetic effects come dangerously close to blurring the lines between network warfare and conventional warfare, in which case demonstrating such capabilities runs the risk of escalation into conventional or even nuclear war, depending on the quality of the adversary involved. The fact that such devastating attacks do not happen may, ironically, be evidence that a higher-level form of deterrence is working with respect to worst-case scenarios such as the one described in the

Solarium article cross the threshold into the use of armed force. But this form of deterrence operates due to the prospect of escalation to physical conflict, rather than any signaling or demonstration of cyber capabilities.

In order for signaling to an adversary with a coercive purpose to work, one must convey to the adversary both a strong enough capability and sufficient credibility. The reason deterrence worked in the Gulf War is that U.S. policymakers had a well-established and highly feared capability in hand, and establishing credibility was the primary concern in that scenario. Ambiguously suggesting nuclear weapons use had a deterring effect on the possibility of escalation, even if there was no overt threat of their being used. However, cyber-based capabilities have not reached a potency such that they alone could coerce an adversary. The failure of the coalition to compel Saddam to withdraw from Kuwait underscores the limits of compellence even when based on overwhelming conventional force; cyber capabilities are still not comparable to conventional forces in hurting power, which undermines their viability for coercion. Credibility is not an issue; the history of cyber conflict demonstrates that the only way nations establish capability is by the actual employment of capabilities against adversary targets, which solves the problem of credibility. Similar to the nuclear analogy, no one can really doubt the publicly demonstrated capabilities of the U.S. in cyberspace, based on the Stuxnet attack and the Snowden intelligence breach. Yet the most powerful cyber effects on critical infrastructure, such as those demonstrated in the Stuxnet attack, cannot permanently disarm an adversary and run the risk of escalation into a kinetic war. Research for this thesis indicates that signaling in cyberspace to an adversary for the intent of coercion is possible, but unlikely to succeed while cyberweapons lack the capability to inflict sufficient harm on the adversary.

B. PERSISTENT ENGAGEMENT

1. Overview

The 2018 Department of Defense Cyber Strategy adopted a strategy that seeks to create cyber security through, among other things, persistently contesting malicious activity in cyberspace through day-to-day competition, reinforcing norms of responsible

state behavior in cyberspace, and adopting a stance of defending forward in order to shape cyberspace to the advantage of the US [35]. This concept was depicted by Michael Fischerkeller and Richard Harknett, who argue for a strategy of persistent engagement in cyberspace by constantly contesting enemy cyber organizations and lines of effort on their own "cyber terrain," with the goal of shifting the strategic environment in favor of the United States [51]. Persistent engagement embraces the concept that nations will consistently act in cyberspace short of the threshold of armed conflict, and that cyber warfare is most used to achieve strategic goals through espionage, sabotage, and subversion [40]. Fischerkeller and Harknett state that the interconnectedness and constant communication between systems that characterize the Internet, along with the absence of traditional concepts of national sovereignty, encourage the concept of persistent contact and engagement [40]. This strategy was demonstrated by the previously discussed actions taken by U.S. CYBERCOM that preemptively shut down the Russia-based IRA to prevent their influence operations on the 2018 elections. This strategy views cyberspace as a domain in which conflict between nations is the rule, not the exception, at least on a level below the use of armed force.

Persistent engagement is effectively a rejection of a coercion strategy, and any signaling that may take place is purely coincidental as a result of ongoing cyber operations. Since none of these activities cross the threshold of armed force or justify a devastating response, deterrence is not a viable strategy, because it is unlikely any adversary will use cyber capabilities to achieve that kind of destructive effect.

The 2020 Solarium Commission, a commission by the U.S. government to determine how the U.S. should frame its national cyberspace strategy for the future, decided to further build on the idea of persistent engagement and incorporate it into a strategy of "layered" cyber deterrence [3]. The layers of this deterrence are the integration of the efforts of the government, the private sector, and the citizens of the U.S. to form a whole-of-nation strategy of 'deterrence by denial' to reduce the benefits and increase the costs of adversary attempts to attack the U.S. in cyberspace [3]. The three pillars of this strategy are shaping behaviors and norms on the international stage for cyberspace, denying the benefits of adversary actions, and imposing costs on adversaries should they violate

those norms [3]. Friction and persistence engagement fits into this strategy in the shaping of norms and imposing costs, by stopping malicious activity in cyberspace close to the source to render the effects of the attack harmless and punish adversary activity accordingly [3].

Here is where clarity on the concept of deterrence is important. The prerequisite for a strategy of "deterrence by denial" is reliable defense based on capabilities that provide protection against any enemy attack. As discussed in Chapter I, an attacker viewing the defensive capabilities of their intended target could be deterred from attacking at all, but this is a secondary effect of sufficient defense, and a confident defender might even perceive advantages of allowing the adversary to attack. Deterrence by denial is therefore more of an adjunct to persistent engagement than is deterrence relying on coercion through threat of punishment, which has been the focus in this thesis.

2. Persistent Engagement and Signaling

The Solarium Commission recommended implementing a coherent strategy of signaling for a strategy of comprehensive deterrence that spans cyber and kinetic domains, a key element of deterrence connectivity missing from the 2018 DOD Cyber Strategy [3]. Conducting operations without overt messaging from U.S. government authorities could easily be mistaken for outright aggression and cause unintentional escalation that may lead to kinetic conflicts [3]. Signaling, therefore, should involve the coordination of various instruments of power, not just operations and actions in cyberspace. The Solarium report also advocates that a multi-tiered strategy of signaling be adopted, with strategic signaling following one policy, and tactical/operational signaling following another. The strategic level of signaling should be overt in nature, using traditional means of strategic signaling with the goal of as much transparency as possible when it comes to ways that the U.S. will respond to attacks above the threshold of armed conflict, something that the U.S. has not done before [3]. It also highlights the need to account for the use of force below the threshold of armed conflict, though it does not recommend how to do so. The tactical and operational levels of signaling should remain covert or clandestine, and potentially entail the use of non-cyber means to deter adversary cyber campaigns that do not meet the

threshold of armed conflict [3]. The Commission also acknowledged the need for clearly articulated consequences tied to adversary activity both above and below the threshold of war, as well as a framework for self-attribution of cyber operations should that be necessary to convey credibility [3].

As previously noted, the Solarium Commission imprecisely uses the term "deterrence" in concert with a policy of persistent engagement, as deterrence and compellence involve the latent threat of violence or force, rather than the constant application of it. However, the strategy of persistent engagement suggests a more viable adaption of cyber capabilities and signaling to the cyber environment, specifically at the operational and tactical levels. Persistent engagement acknowledges that, below the level of armed conflict, cyber capabilities do not have the coercive power necessary to alter the calculus of an adversary, and that the benefits of using cyberspace to accomplish strategic objectives outweigh the potential punishment from a symmetric retaliation of a cyber capability. In the words of Fischerkeller and Harknett, "In, through, and from cyberspace, adversaries will act persistently short of armed conflict" [52]. The full array of traditional and unconventional tools of power are necessary for achieving coercion. In light of persistence, signaling in cyberspace becomes "nested" within larger campaigns of coercion, along with conventional military capabilities, economic influence, and diplomatic overtures.

The overt, strategic signaling talked about in the Solarium Commission attempts to address some of the problems inherent in using persistent engagement as a strategy, but also seems contradictory on the issue of establishing thresholds of response for activities below the level of armed conflict. First, it articulates the need for clear communication in light of the fact that the posture of defending forward and persistently contesting the enemy in both neutral and adversary cyberspace has offensive aspects to it. Clear communication is necessary to prevent the adversary from viewing the operations as escalatory. Second, the idea of clearly communicating or establishing a threshold of retaliation in cyberspace has been missing in past strategies, and was not attempted in any of the cases of cyber conflict studied in Chapter II.

At first glance, the need to communicate in order to avoid escalation seems to correctly account for the trajectory of cyber conflict, in that the employment of cyber capabilities seems to be escalatory in nature and seems to result in victims developing and retaliating with their own cyber capabilities. Persistent engagement, following the principle that conflict in cyberspace is a constant, might be viewed as escalatory without the necessary messaging from the U.S. government. However, the fact that persistent engagement assumes that adversaries will be using cyberspace to achieve their own strategic goals, regardless of what the U.S. does in cyberspace to stop them, raises the question of whether or not signaling will have any impact on adversary actions in the first place. It may help with any neutral or allied partners who are impacted by such a strategy to communicate why consequences, if any, occurred within their IP space. However, communicating to avoid escalation, short of the threshold of armed conflict, seems to be a concept inconsistent with the stance of persistent engagement, though not of deterrence. If U.S. CYBERCOM reverted back to a stance of achieving deterrence, rather than persistently contesting activity, then it may be of great value to see whether establishing "red lines" and consistently enforcing those thresholds has an observable impact on adversary cyber activity. The cumulative effect of "imposing costs" in cyberspace may have a long-term strategic effect of signaling to adversaries the resolve and dedication of the U.S. to shaping the norms of cyberspace behavior, especially if used in concert with other coercive tools such as sanctions, but that is not evident at this point in time.

The greatest utility of signaling with cyber capabilities in an environment of persistent engagement may likely be found in support of crisis management or short-term deterrence at the operational level and tactical level. Even if cyber capabilities do not seem to have the coercive power by themselves to deter or compel, they may still be used to signal or brandish capabilities in a supporting role to other military, economic, or diplomatic overtures, in both an overt and covert capacity. One such example of the effectiveness of cyber capabilities used in a supporting role to kinetic capabilities is Operation Orchard. This was an attack by the Israelis against a developing nuclear program built by the Syrians [53]. When the Israelis discovered that the Syrians were attempting to construct a nuclear development facility, they decided to launch a kinetic strike against the

target. On September 6, 2007, the Israeli Air Force sent a flight of tactical aircraft that successfully attacked and destroyed the facility. During the mission, there was no attempt by the Syrians to shoot them down, because Israeli cyber operatives had successfully penetrated the Syrian IADS (Integrated Air Defense System) network and injected a false picture of clear skies to the adversary radar and missile operators [53]. While not an example of overt signaling, the demonstrated effectiveness of using cyber capabilities to support an airstrike does open up the possibility of using such capabilities to credibly signal resolve to an adversary. Using cyber capabilities against adversary military targets while simultaneously brandishing conventional military power could help to effectively persuade an adversary that the opening shots of any kinetic exchange would not end in their favor.

Another example of how cyber capabilities were used in concert with military forces is the U.S. response to Iran's shootdown of a drone in the summer of 2019. After planning and then backing away from the use of conventional strikes to retaliate for the attack, the Trump administration then ordered USCYBERCOM to conduct cyber strikes against an IRGC (Iranian Revolutionary Guard Corps) database that was allegedly being used to plan attacks against oil tankers in the Arabian Gulf, though initial open source reports stated that the attacks were directed against IRGC missile command-and-control systems [54]. This coincided with the deployment of additional U.S. Navy ships to the Gulf. This response was deemed as being proportionate, as opposed to the cancelled conventional strikes that would have resulted in destruction and loss of life [54]. Around the same time the attacks occurred, the DHS (Department of Homeland Security) did warn of increased Iranian malicious activity against U.S. critical industries, potentially out of fear of Iranian counter-reprisals, but also in light of the overall trend of increased Iranian activity in cyberspace [54].

These two examples shed light on how cyber capabilities can be used to signal for crisis management and short-term deterrence. Cyber capabilities can be successfully used to augment conventional military deterrence signaling in a non-escalatory manner. The very fact that cyber effects are non-lethal and temporary, but can still enable and support effects that are lethal, means that they can be used to convey both a credible threat and resolve for escalation to kinetic actions without being escalatory in and of themselves. The

attack on the IRGC certainly wasn't able to deter Iran from continuing its disruptive efforts in cyberspace [54], and it is almost impossible to prove if deterrence is working in a kinetic sense, because there may be a myriad of other factors at play that cause an adversary to withhold violence. However, it provided U.S. policymakers a way to avoid armed conflict while being able to demonstrate resolve and hold Iran accountable. It would be no stretch to imagine a similar scenario, where Iran attempts to close the Strait of Hormuz, and the U.S. could respond by deploying a carrier strike group to the Arabian Gulf while using a cyber capability to neutralize their IADS, similar to the scenario in Operation Orchard. Using a cyber capability that achieved such an effect may help make the threat of conventional force more credible. Though speculatory, the fact that the U.S. is "burning" a given vulnerability to penetrate Iranian military networks in a crisis could send a message to the Iranians that, not only is the U.S. serious enough about the situation to spend that kind of resource, but also that the U.S. might have more hidden exploits available in the case of an actual conflict and can still adversely affect the Iranians should the crisis continue or escalate into a kinetic confrontation. Additional depth of commitment is conveyed in this kind of scenario, because the effects of any such cyberattack are meant to be accurately attributed to the attacker, and therefore any discussion about concealing the exploits is likely moot.

Finally, cyber signaling in an environment of persistent engagement could potentially be used for overt and covert signaling to convey resolve and intent, rather than just for coercive purposes. USCYBERCOM has already overtly signaled resolve and intent to the Russians, through its willingness to openly self-attribute its role in Operation Glowing Symphony [38], the shutdown of the IRA [37] and the deployment of personnel to Montenegro [39].

This prospect is supported by evidence of successful signaling using non-lethal actions in other domains. Austin Carson and Keren Yarhi-Milo conducted a study for how covert action can be used by nations to signal resolve and intentions, specifically focusing on the Cold War proxy conflicts in Angola and Afghanistan [55]. They found that the use of covert aid, whether in the form of funding or the shipment of arms, showed success being used to signal commitment and resolve to strategic adversaries as well as concerned

third-party nations, all while attempting to account for political sensitivities on the domestic level [55].

In Angola, both the Soviet Union and the United States inferred mostly the correct messages that each wished to send each other based on the fact that arms and funding provide hard evidence of commitment to a cause [55]. The study found that the increase in Soviet covert aid to the Communist efforts in Angola was an effort to signal both the United States and China of the willingness of Moscow to support its Allies, in light of a supposed invasion by South Africa (supported by Washington) of Angola. The U.S. response to increase covert aid was because they perceived, correctly, the Soviet signaling attempt. This was in turn viewed as a signal by the Soviets as a message that the U.S. was committed to winning in Angola [55].

In Afghanistan, Carson and Yarhi-Milo's study found that the U.S. perceived the increased covert involvement of the Soviets as a means of not just shoring up its allies in Afghanistan, but testing the U.S. resolve in resisting increased Soviet assertiveness on the world stage, a conclusion backed up by intelligence reports at the time [55]. As a result, the decisionmakers concluded that it was "imperative that we not only act to counter what the Soviets have done in Afghanistan, but be perceived as doing so" [55]. Covert aid was necessary to provide the Pakistani leadership cover for not overtly working with Americans, but once arms shipments began arriving and causing Soviet casualties, they sent a message to the Soviets about the commitment of the U.S. to punish increased aggression in the Third World [55]. It also signaled to the Pakistanis that the U.S. had not abandoned them to the Soviet Union [55].

While signaling was not the only intention of these adversaries in providing support, it was a primary concern on both sides [55]. Because of the covert nature of many cyber operations, cyber effects and capabilities may be ideally suited for the purpose of covert signaling. The case studies of Chapter II demonstrate that states already infer adversary intentions by the mere use of cyber capabilities. Cyber brandishing could provide a unique set of tools for policymakers to signal adversaries, with a range of options from increased presence on networks of interest to a deployment of USCYBERCOM personnel to support an ally, similar to the support that was provided by the U.S. to Montenegro [39].

Over all, cyber signaling seems to be more useful as a coercive tool in a strategy of persistent engagement, rather than a strategy of deterrence. The Solarium Commission's desire for overt strategic communication concerning thresholds for retaliation does seem to address the flaws of past deterrence strategies (or lack thereof), but it still does not account for the inefficacy of deterrence in cyberspace below the threshold of armed conflict. Any cyberattack that constitutes a use of armed force would be met and responded to in the same framework that any other armed attack would be. But establishing thresholds for response below a state of armed conflict seems to inherently contradict a strategy that entails constant friction and defending forward, and assumes that adversaries will not be deterred from using cyberspace to achieve strategic goals. Persistent engagement renders concept of signaling for deterrence against adversary activity in cyberspace obsolete. The utility of signaling and brandishing cyber capabilities seems to be found in use as a supporting element to other instruments of coercion, as well as potentially being useful for covert and overt signaling of resolve and commitment to adversary nations.

C. CONCLUSION

Martin Libicki and Jason Healy highlighted the potential difficulties of implementing a capabilities-based strategy of strategic cyber deterrence and brandishing cyber capabilities to create deterrence. Libicki pointed out that the impact of brandishing capabilities was highly dependent on the nature of the system that is targeted, as well as the qualities of the adversary, and would likely be an unreliable foundation on which to base deterrence [1]. He brought up the possibility that the demonstration of cyber capabilities may actually undo their potential impact, based on the fact that the adversary would know how to patch whatever vulnerability was exploited. Finally, he also pointed out that the temporary and non-lethal nature of cyberattacks may also undermine the coercive power of signaling in cyberspace [1]. Jason Healy added to these concerns by stating that nations seem to demonstrate cyber capabilities by employing them against real targets, and that such demonstrations only lead to escalation, not deterrence [14].

The history of cyber conflict evaluated in this thesis supports Healy's and Libicki's fears that using cyber capabilities only leads to escalation. The various attempts at coercion

in the Gulf War highlight the relative importance of credibility and capability in signaling, and how cyber capabilities have not demonstrated the coercive power needed to alter an adversary's calculus. If attribution, holding adversary assets at risk, and doing so repeatedly are what are needed to created deterrence, the analysis of this thesis has shown why cyber capabilities fall short in the second aspect. Based on the temporary and non-lethal nature of cyber capabilities as they exist today, it is unlikely that such signaling efforts would result in deterrence or be useful for compellence. Even if cyberattacks could achieve that kind of coercive power, they would come dangerously close to escalating into the realm of armed conflict.

Persistent engagement is more consistent with the environment of cyberspace, and concedes that adversaries will continue to act in their own strategic interests short of the level of armed conflict, regardless of the credibility of the U.S. or its capabilities in wielding cyberweapons. The concept of defending forward and contesting the adversary in neutral or on its own cyber terrain foregoes the need for brandishing cyber capabilities to create deterrence. The future utility of cyber capabilities seems to entail the integration of cyber instruments of power with traditional forms of coercion, such as the parallel brandishing and employment of cyber capabilities with conventional military power. Used as such, cyber capabilities may prove useful in crisis management or creating short-term deterrence. Cyber signaling may also be useful in conveying strategic resolve and intent to peer adversaries as well as important third parties. As such, this thesis recommends that the U.S. government continue orienting its strategy in cyberspace toward one of persistent engagement, and, in light of that strategy, brandishing cyber capabilities in the very specific contexts in which such demonstration can have positive effects.

Recommendations for further research are to determine if the long-term application of a strategy of persistent engagement, used in concert with other national instruments of power, may result in successful coercion of adversaries to conform to desired norms of behavior in cyberspace. Further research into the potential effectiveness of cyber capabilities in the future would also be helpful.

LIST OF REFERENCES

[1] M. C. Libicki, “Brandishing Cyber Capabilities,” RAND Corporation, Arlington, VA, USA, 2013.

[2] S. G. Fogarty and B. N. Sparling, “Enabling the Army in an Era of Information Warfare,” *Cyber Defense Review*, vol. 5, no. 2, pp. 17–26, 2020.

[3] U.S. Cyberspace Solarium Commission, “Report,” Washington, DC, USA, 2020.

[4] C. F. Wrenn, “Strategic Cyber Deterrence,” Proquest LLC, Ann Arbor, MI, USA, 2012.

[5] T. C. Schelling, *Arms and Influence*, New Haven, CT, USA: Yale University Press, 1966.

[6] NATO, *The North Atlantic Treaty*, Washington, DC, USA, 1949.

[7] M. C. Libicki, *Cyberspace in Peace and War*, Annapolis, MD, USA: Naval Institute Press, 2016.

[8] B. L. Connelly, S. T. Certo, R. D. Ireland and C. R. Reutzel, “Signaling Theory: A Review and Assessment,” *Journal of Management*, vol. 37, no. 1, pp. 39–67, 2011.

[9] M. C. Libicki, “Cyberdeterrence and Cyberwar.” RAND Corporation, Arlington, VA, USA, 2009.

[10] R. Langner, “To Kill a Centrifuge: A Technical Analysis,” The Langner Group, Arlington, VA, USA, 2013.

[11] J. M. Park, “Finding Effective Responses against Cyber Attacks for Divided Nations,” Naval Postgraduate School, Monterey, CA, USA, 2015.

[12] W. Hoffman, “Is Cyber Strategy Possible?,” *The Washington Quarterly*, vol. 42, no. 1, pp. 131–152, 2019.

[13] D. E. Sanger, “Obama Ordered Sped Up Wave of Cyberattacks against Iran,” *New York Times*, 1 June 2012. [Online]. Available: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[14] J. Healy, “The Cartwright Conjecture,” in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, New York, NY, USA, Brookings Institution Press, 2016, pp. 173–194.

[15] T. Brewster, “‘Bone-Chilling’ Research Suggests Iran Gearing Up to Avenge Stuxnet Hacks,” Forbes, 14 December 2014. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2014/12/02/bone-chilling-research-suggests-iran-gearing-up-to-avenge-stuxnet-hacks/#1382d2a921f8

[16] S. W. Harold, M. C. Libicki and A. S. Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica, CA, USA: RAND Corporation, 2016.

[17] Z. Noble, “Time to Consider the ‘Hack-back’ Strategy?,” FCW Magazine, 30 September 2015. [Online]. Available: https://fcw.com/articles/2015/09/30/hack-back-strategy.aspx

[18] M. Connell and S. Vogler, “Russia’s Approach to Cyber Warfare,” Center for Naval Analyses, Arlington, VA, USA, 2017.

[19] R. J. Deiber, R. Rohozinski and M. Crete-Nishihata, “Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War,” *Security Dialogue*, vol. 43, no. 1, pp. 3–24, 2008.

[20] S. P. White, “Understanding Cyberwarfare: Lessons from the Russia-Georgia War,” Modern War Institute, West Point, NY, USA, 2018.

[21] S. P. White, “Subcultural Influence on Military Innovation: The Development of U.S. MIlitary Cyber Doctrine,” Harvard University, Cambridge, MA, USA, 2019.

[22] United States Cyber Command, “U.S. Cyber Command History,” Accessed 29 November 2020. [Online]. Available: https://www.cybercom.mil/About/History/

[23] R. Hughes, “A Treaty for Cyberspace,” *International Affairs*, vol. 86, no. 2, pp. 523–541, 2010.

[24] Agence France-Presse Agence, “Defence Talk,” 11 January 2010. [Online]. Available: https://www.defencetalk.com/skorea-to-launch-cyber-warfare-command-23649/

[25] A. Cherepanov, “Certificates Stolen from Taiwanese tech-companies Misused in Plead Malware Campaign,” welivesecurity, 9 Jul 2018. [Online]. Available: https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/#:~:text=Stuxnet%20used%20digital%20certificates%20stolen,evidenced%20by%20this%20recent%20discovery

[26] B. M. Jensen and B. Valeriano, “From Arms and Influence to Data Manipulation: What Can Thomas Schelling Tell Us about Cyber Coercion,” Lawfare, 16 March 2017. [Online]. Available: https://www.lawfareblog.com/arms-and-influence-data-and-manipulation-what-can-thomas-schelling-tell-us-about-cyber-coercion

[27] H. Farrell, “The Political Science of Cybersecurity IV: How Edward Snowden Helps U.S. Deterrence,” Washington Post, 12 March 2014. [Online]. Available: https://www.washingtonpost.com/news/monkey-cage/wp/2014/03/12/the-political-science-of-cybersecurity-iv-how-edward-snowden-helps-u-s-deterrence/

[28] “Look Who’s Listening,” *The Economist,* vol. 407, no. 8840, pp. 23–25, 2013.

[29] A. F. Brantly, N. M. Cal and D. P. Winkelstein, “Defending the Borderland: Urkainian Military Experiences with IO, Cyber, and EW,” Army Cyber Institute at West Point, West Point, NY, USA, 2017.

[30] P. Polityuk, “Ukraine Sees Russian Hand in Cyber Attacks on Power Grid,” Reuters, 12 February 2016. [Online]. Available: https://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E

[31] D. Goodin, “First Known Hacker-Caused Power Outage Signals Troubling Escalation,” ArsTechnica, 4 January 2016. [Online]. Available: https://arstechnica.com/information-technology/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

[32] C. Lam, “A Slap on the Wrist: Combatting Russia’s Cyber Attack on the 2016 U.S. Presidential Election,” *Boston College Law Review,* vol. 59, no. 6, pp. 2167–2201, 2016.

[33] Office of the Director of National Intelligence, “Assessing Russian Activities and Intentions in Recent U.S. Elections,” Office of the Director of National Intelligence, Washington, DC, USA, 2017.

[34] M. Isikoff and D. Corn, “’Why the Hell Are We Standing Down?’,” Mother Jones Daily, 9 March 2018. [Online]. Available: https://www.motherjones.com/politics/2018/03/why-the-hell-are-we-standing-down/

[35] Department of Defense, “Department of Defense Cyber Strategy Summary,” Department of Defense, Washington, DC, USA, 2018.

[36] E. Nakashima, “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms,” Washington Post, 11 July 2020. [Online]. Available: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

[37] E. Nakashima, “Trump Confirms Cyberattack on Russian Trolls to Deter Them During 2018 Midterms,” Washington Post, 26 February 2019. [Online]. Available: https://www.washingtonpost.com/national-security/trump-confirms-cyberattack-on-russian-trolls-to-deter-them-during-2018-midterms/2020/07/11/66a845e8-c2c3-11ea-b178-bb7b05b94af1_story.html

[38] D. Temple-Raston, “How the U.S. Hacked ISIS,” NPR, 26 September 2019. [Online]. Available: https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

[39] P. M. Nakasone and M. Sulmeyer, “How to Compete in Cyberspace,” Foreign Affairs, 25 August 2020. [Online]. Available: https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity

[40] M. P. Fischerkeller and R. J. Harknett, “Deterrence Is Not a Credible Strategy for Cyberspace,” *Orbis*, vol. 61, no. 3, pp. 381–393, 2017.

[41] S. D. Sagan, “The Commitment Trap: Why the U.S. Should Not Use Nuclear Threats to Deter Biological and Chemical Weapons Attacks,” *International Security*, vol. 24, no. 4, pp. 85–115, 2000.

[42] B. Scowcroft and G. H. W. Bush, *A World Transformed*, New York, NY, USA: Knopf, 1998.

[43] J. A. Baker, The Politics of Diplomacy: Revolution, War, and Peace, 1989–1992, New York, NY, USA: G.P. Putnam’s Sons, 1995.

[44] T. Sauer, “A Second Nuclear Revolution: From Nuclear Primacy to Post-existential Deterrence,” *Journal of Strategic Studies*, vol. 32, no. 5, pp. 745–767, 2009.

[45] J. G. Stein, “Deterrence and Compellance in the Gulf,1990-91: A Failed or Impossible Task?,” *International Security*, vol. 17, no. 2, pp. 147–179, 1992.

[46] J. Samaan, “Cyber Command: The Rift in U.S. Military Cyber-Strategy,” *The RUSI Journal*, vol. 155, no. 6, pp. 16–21, 2010.

[47] M. Parmar and A. Domingo, “On the Use of Cyber Threat Intelligence (CTI) in the Support of Developing the Commander’s Understanding of the Adversary,” *MILCOM 2019–2019 IEEE Military Communications Conference (MILCOM)*, Norfolk, VA, USA, 2019.

[48] Fireeye, “Advanced Persistent Threat Groups,” Fireeye Technologies, 2020. [Online]. Available: https://www.fireeye.com/current-threats/apt-groups.html#undisclosed

[49] S. Morgan, “Cybercrime Damages $6 trillion by 2021,” Cybercrime Magazine, 16 October 2017. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[50] T. Rogoway and J. Trevithick, “The Night a Mysterious Drone Swarm Descended on Palo Verde Nuclear Power Plant,” The Drive, 29 July 2020. [Online]. Available: https://www.thedrive.com/the-war-zone/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant

[51] M. P. Fischerkeller and R. J. Harknett, “Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation,” Institute for Defense Analysis, Alexandria, VA, USA, 2018.

[52] M. P. Fischerkeller and R. J. Harknett, “Persistent Engagement and Cost Imposition: Distinguishing between Cause and Effect,” Lawfare, 6 February 2020. [Online]. Available: https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.

[53] D. P. Hughes and H. Prunckun, “Archer’s Stakes in Cyber Space: Methods to Analyze Force Advantage,” in *Cyber Weaponry*. *Advanced Sciences and Technologies for Security Applications*, Cham, Springer International Publishing AG, 2018, pp. 71–85.

[54] E. Nakashima, “Trump Approved Cyber-strikes against Iranian Computer Database Used to Plan Attacks on Oil Tankers,” Washington Post, 22 June 2019. [Online]. Available: https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html

[55] A. Carson and K. Yarhi-Milo, “Covert Communication: The Intelligibility and Credibility of Signaling in Secret,” *Security Studies*, vol. 26, no. 1, pp. 124–156, 2016.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California